ESG Research
Final Sponsor Report

The Modernization of Data Protection

By Jason Buffington, Senior Analyst and Bill Lundell, Senior Research Analyst
With Jenn Gahm, Senior Project Manager

April 2012

Contents

List of Figures

Executive Summary

Report Conclusions

ESG conducted an in-depth survey of 330 IT professionals familiar with and/or responsible for data protection solutions (hardware and software) and processes, as well as potential future plans. Survey participants represented midmarket (100 to 999 employees) and enterprise-class (1,000 employees or more) organizations in North America (United States and Canada) and Western Europe (United Kingdom, France, and Germany).

Based on the data collected from this survey, ESG concludes:

- **Increasing data volumes continue to impact data protection strategies.** More than half of midmarket respondents now report total data volumes exceeding 10 TB and 49% of enterprise organizations report more than 100 TB (see Figure 1). The majority (57%) of organizations report annual growth of between 11% and 30% (see Figure 2), which should not be underestimated. Even with a seemingly-modest 20% annual growth rate, an organization with 10 TB of total data would expand capacity requirements by 2 TB in a year while a 100 TB environment would add 20 TB from the previous year. Existing data footprints coupled with steadily increasing growth rates presents ongoing challenges to IT organizations and affects data protection strategies.
- **Organizations continue to face diverse data protection challenges**. When presented with nearly two dozen responses to the question, "what would you characterize as challenges with your organization's current data protection processes and technologies?" every response received at least one vote, demonstrating the variety of data protection issues IT organizations grapple with daily (see Figure 3). Those prioritized as the "primary" data protection challenge are closely associated with data growth: cost(s) (14%), need to reduce backup times (9%), and keeping pace with the capacity of data to protect (8%), and backup hardware costs (7%).
- **Improving disaster recovery (DR) is the top data protection spending initiative for 2012-2013.** This year's top data protection investments are themed around mitigating risk and modernizing data protection tape (see Figure 4). Twenty-eight percent of respondents cited improving DR and 25% noted the need to meet compliance requirements highlighting IT's desire to minimize risk. Improving the backup and recovery of virtual server environments (23%) and the elimination of tape (23%) suggest IT's aspiration to modernize data protection technologies and processes.
- **The business value of data differentiates protection strategies.** All data is not valued equally, as evidenced in users' responses to questions regarding applied data protection strategies and service level agreements (SLAs). For tier-1 data, 53% of respondents could withstand one hour or less of downtime, compared to 21% for tier-2 and only 13% for tier-3 (see Figure 5). The differences between tiers regarding SLAs also become apparent when the overall confidence in the ability to prevent both downtime (see Figure 6) and data loss (see Figure 7), the frequency of backup copies (see Figure 8), and the types of data protection solutions used for each tier (see Figure 9) are examined.
- **Backup isn't as 'broken' as some might presume.** On average, 85% of backup jobs are completing successfully—with 80% of restores completing within SLAs (see Figure 10). While improved backup reliability would be better, the real issue is that one out of five restores fail. In almost all cases, ESG recommends a more rigorous testing methodology for backup technologies and processes, along with transparency by IT to its partners and stakeholders on data protection capabilities and SLAs.
- **The shift from tape to disk continues.** Despite the fact that a mere 10% of organizations use tape as their only backup storage media, tape is still an integral part of many organizations' data protection strategies. In fact, while two-thirds of organizations use disk storage as part of their primary data protection strategy, 56% use tape as a tier at some point in the backup process (see Figure 11). Only 7% of organizations

leverage a third-party cloud service as part of their primary data backup process – 5% use cloud services as another tier, while 2% back up directly over the WAN to a service provider.

- **It is acceptable to have multiple data protection solutions.** Primarily for the purposes of reducing licensing costs across enterprises, as well as integrating data-protection-enabling hardware, not only is backup application diversity active now, this is a trend that will continue in the future. According to Figure 12, 40% of IT environments use a single backup application today. However, within two years, this figure will drop to only 25%. While the prevailing current on-premises deployment model is software deployed on a physical server, nearly half would prefer to either install their backup applications on a virtual appliance or integrate them on a storage system (see Figure 13).
- **Status quo backup solutions are *not* sticky.** Half of survey respondents have had their primary backup application deployed for three years or less (see Figure 14). If hardware is a cornerstone of a backup solution, it presumably has a 3-year reconsideration point with relatively little attractiveness to retain versus an alternative hardware vendor. If the backup solution is software-centric, there are more frequent chances to renew commitment with the customer (or lose it), based on capabilities and TCO. The cost and time invested in acquiring, deploying, and fine-tuning backup applications, as well as training staff to use them, has traditionally inspired fidelity to a particular backup vendor and/or solution. However, if presented with the opportunity to re-architect backup processes, 44% would use a new backup solution/vendor and 16% would use a cloud-based backup service (see Figure 15). According to Figure 16, the top two drivers for changing the status quo are the volume of data organizations have to back up and software licensing models.
- **Non-traditional backup technologies continue to gain momentum.** Advanced technologies such as snapshot, replication, and continuous data protection (CDP) have made impressive strides in terms of adoption. Specifically, more than half currently use snapshot (58%) and/or replication (55%), while 21% use CDP technology (see Figure 17). Array-based solutions were or will be added to existing backup solutions based on how their capabilities enable cost-reduction, regardless of the promise of better SLAs such as faster restores or reduced server overhead. In fact, when considering the predisposition to diversify backup solutions, this is the most likely investment area.
- **Snapshot and replication technologies are replacing—or augmenting—existing backup solutions**. Snapshot and replication are more often becoming likely candidates to replace traditional backup, with 13% of organizations electing snapshot over traditional backup, 28% using replication in lieu of file-level backup, and 20% phasing out backup with a combination of snapshot and replication software (see Figure 18). More than one-quarter of current and planned users of snapshot or replication technology expect to use these solutions in an additive manner with their existing backup applications.
- **Improved RTOs and RPOs are the biggest selling points for snapshot.** When current users were asked about the impact—good or bad—snapshot has had on data protection processes, improved recovery time objectives and improved recovery point objectives were at the top of the list, and while 28% reported increased disk storage capacity requirements, only 13% had experienced increased costs (see Figure 19). Forty-two percent of planned adopters expect to implement snapshot technology via file system (see Figure 20). Despite the fact that very few current users attributed increased costs to snapshot solutions, more than one-third of those respondents with no plans to use snapshot cite cost as an adoption impediment (see Figure 21).
- **Using replication as a stepping stone to disaster recovery.** Forty-two percent of current replication users believe the technology has affected their organization for the better by enabling disaster recovery (see Figure 22). More than one-third of planned adopters expect to implement replication technology via a storage array (see Figure 23). As was the case with snapshot technology, cost was the number one barrier to replication adoption. Specifically, Figure 24 reveals that almost half of those organizations with no plans to implement replication technology cite cost as at least one of the reasons behind the decision.

- **Deduplication is a "when," not an "if."** With disk-based protection being the primary line of defense for most environments, IT is struggling not only with primary storage growth but also backup target growth that is often a multiple of the primary. More than three-quarters of respondent organizations either currently use deduplication or expect to implement the technology within the next 24 months (see Figure 25). Of the many purchase considerations, cost, ease of deployment/use, and impact of backup/recovery performance were ranked in the top three by both current users and planned adopters (see Figure 26). Deduplication is more likely to be implemented in backup software by current users, while planned adopters expect to deploy the technology via an appliance or disk-based storage system (see Figure 27).
- **IT would like to move toward a unified strategy for physical and virtual server protection.** Since organizations deploy server virtualization in phases, a level of heterogeneity exists between physical and virtual workloads. Most respondent organizations (53%) currently use separate backup applications to protect data residing on physical and virtual machines (see Figure 28). However, when respondents were queried on their *preferred* approach, more than two-thirds cited a preference for a single backup application for both physical and virtual environments. So, while IT is willing to diversify data protection solutions (as seen in Figure 12), adding one specifically for virtualization solutions does not appear as a preference.
- **Virtualization protection methods vary greatly—and everyone is relatively happy**. Respondents cite a mix of techniques to protect data in virtual machines. While agent-based solutions are still most popular, a range of host-based, hypervisor-enabled and array-powered backup solutions are all in use (see Figure 29). Most respondents are at least satisfied with their organization's primary method for backing up virtual machines—regardless of the methodology in use—and almost one-in-five report being very satisfied (see Figure 30).
- **The cloud is establishing a foothold as a backup storage tier.** While only 7% of organizations currently use cloud as part of their primary data protection process (as seen in Figure 11), sixteen percent would use cloud services if given the opportunity to completely re-architect their backup processes (as seen in Figure 15). However, the real opportunity is the emerging cloud storage tier: more than one-fifth of organizations currently utilize third-party online backup services to support data protection operations and an additional 23% are evaluating these services (see Figure 31). While—on average—only 5% of total backup data resides on cloud storage today, this number is expected to more than triple over the next two years (see Figure 32). Among both current and planned users of cloud backup, the ability to store data remotely for disaster recovery purposes, improved cost-effectiveness, and simplified budgeting were the three most cited adoption drivers for these services (see Figure 33).

Introduction

Research Objectives

In order to assess the current state of the data protection market, ESG recently surveyed 330 North America- and Western Europe-based senior IT professionals representing midmarket (100 to 999 employees) and enterprise-class (1,000 employees or more) organizations. All respondents were familiar with and/or personally responsible for evaluating, purchasing, or managing data protection technologies—such as backup and recovery software, data replication software, and disk or tape storage systems used for secondary data storage—for their organization.

The survey was designed to answer the following questions:

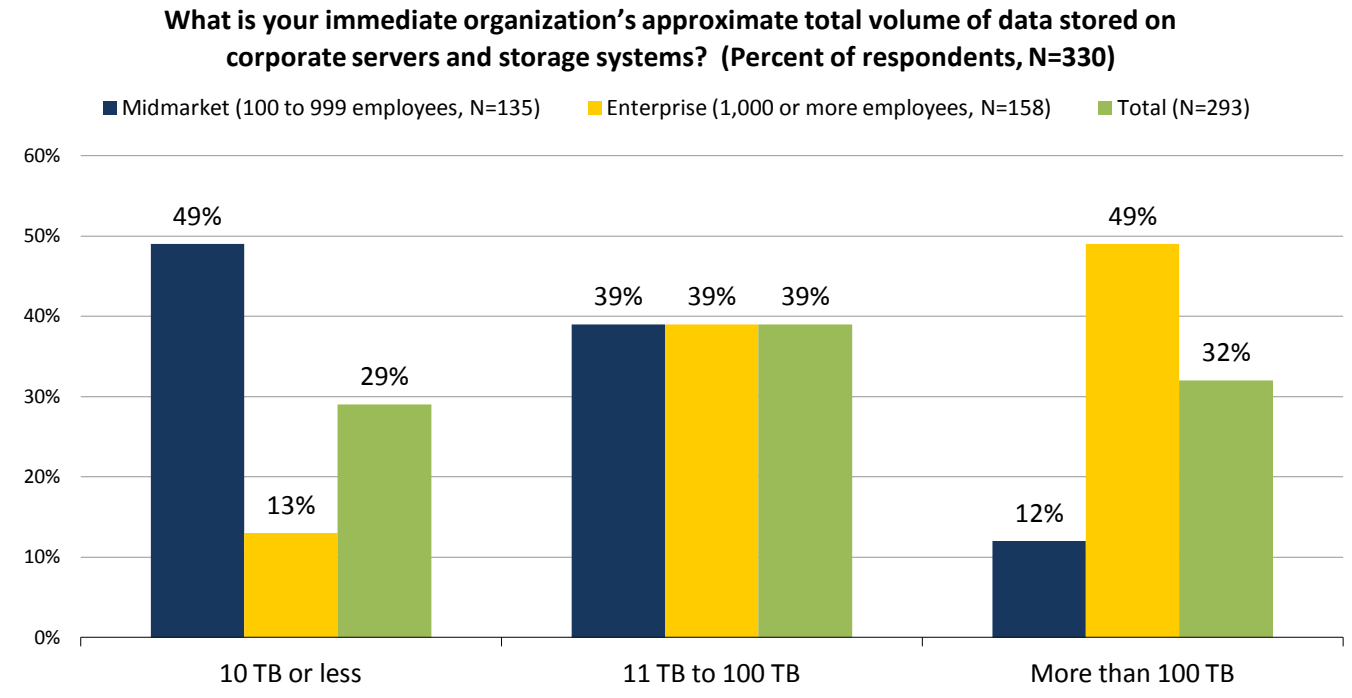
- What are the primary data protection challenges that organizations are currently facing?
- Which areas of data protection will merit the greatest level of investment in 2012 and beyond?
- How confident are organizations that their data protection applications and processes are adequately protecting their data?
- Which types of data protection technologies and processes are currently in use? How will this change going forward?
- What impact does the business value of data have on data protection applications and processes?
- How satisfied are organizations with their current data protection technologies and strategies?
- What types of storage media are currently used to support data protection requirements and how will this change over time?
- How pervasive has data deduplication usage become over the last several years?
- What methods do organizations use to protect virtual machines today?
- Does the organization maintain different approaches to protecting its virtual and physical servers? What is the preference for protecting physical versus virtual?
- What impact is the cloud having on data protection strategies today and how will this change in the near future?

Survey participants represent a wide range of industries including manufacturing, financial services, communications and media, health care, retail, government, and business services. For more details, please see the *Research Methodology* and *Respondent Demographic* sections of this report.

Research Findings

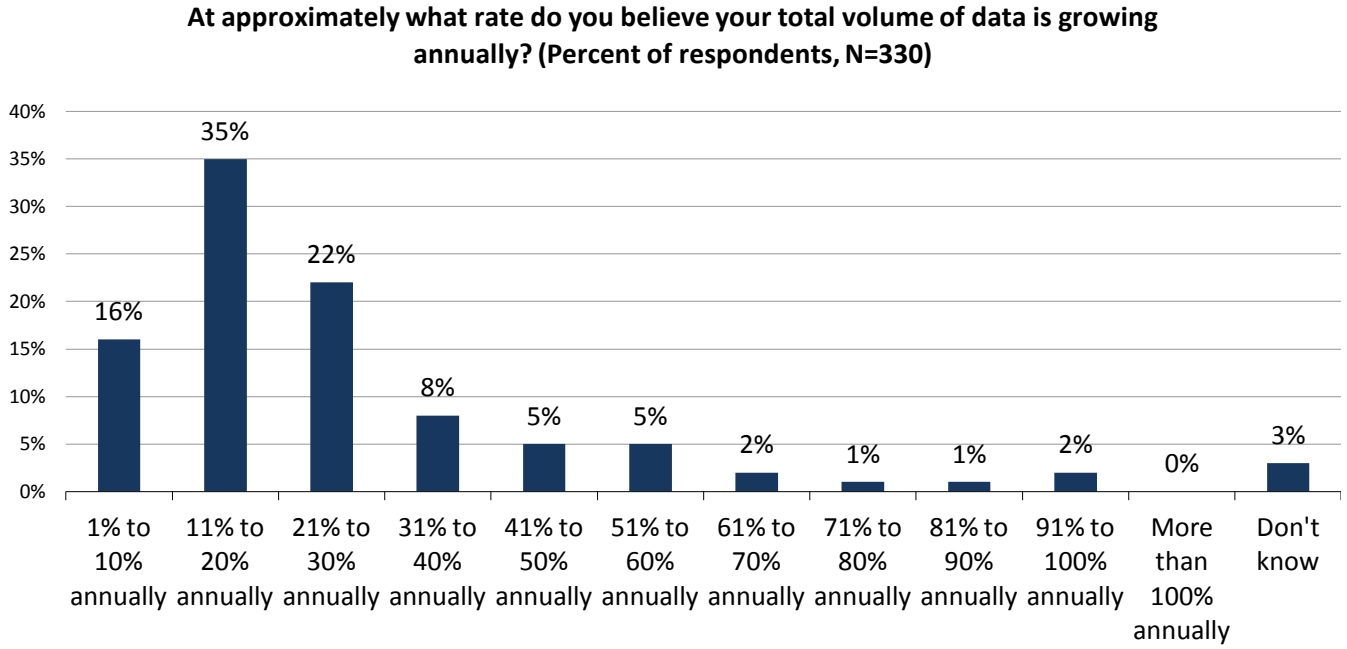
Size and Growth of Data Protection Environments

Figure 1. Total Volume of Data Stored on Corporate Servers and Storage Systems



Source: Enterprise Strategy Group, 2012.

Figure 2. Annual Data Growth Rates

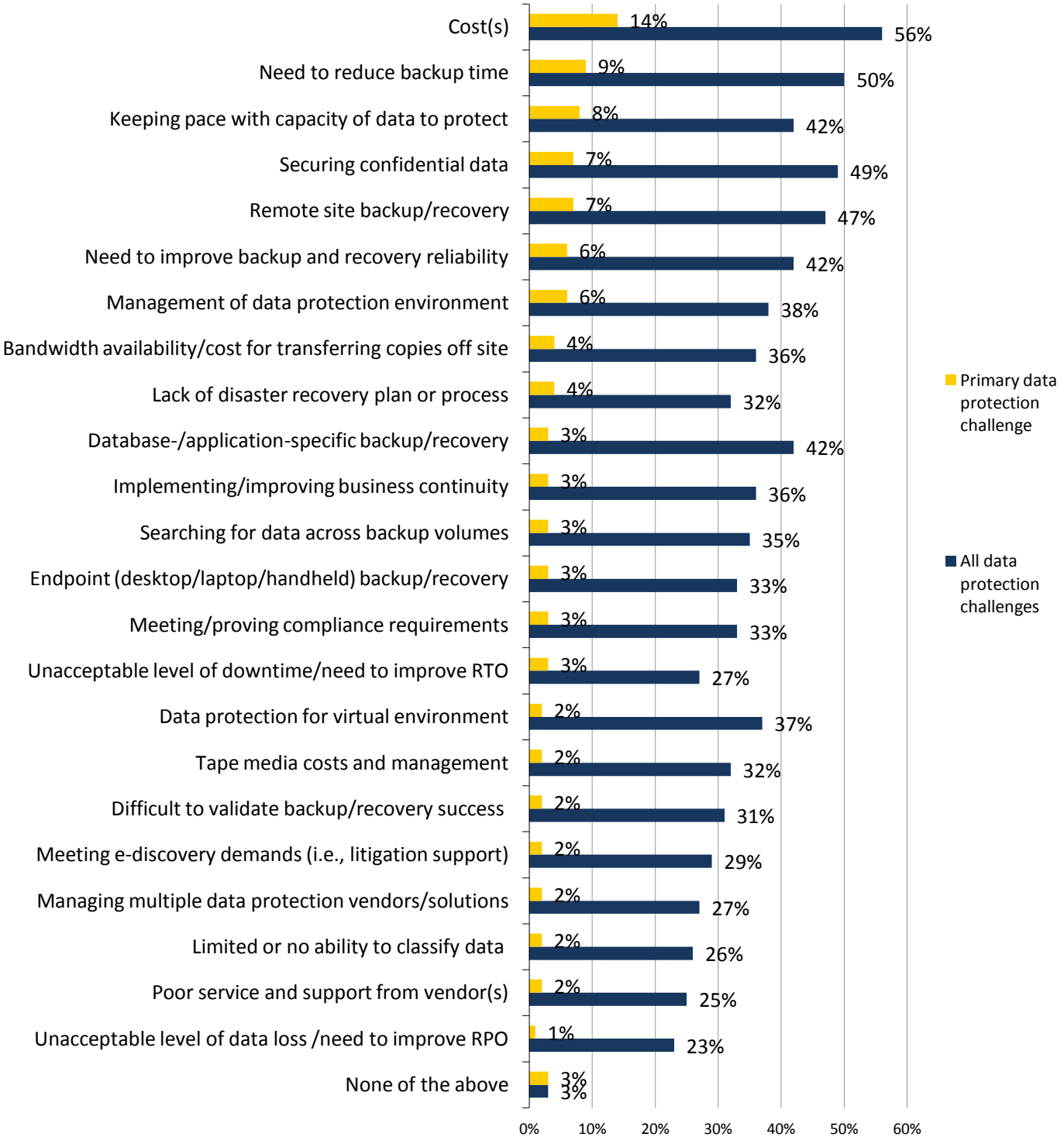


Source: Enterprise Strategy Group, 2012.

Data Protection Challenges and Areas of Investment

Figure 3. Current Data Protection Process and Technology Challenges

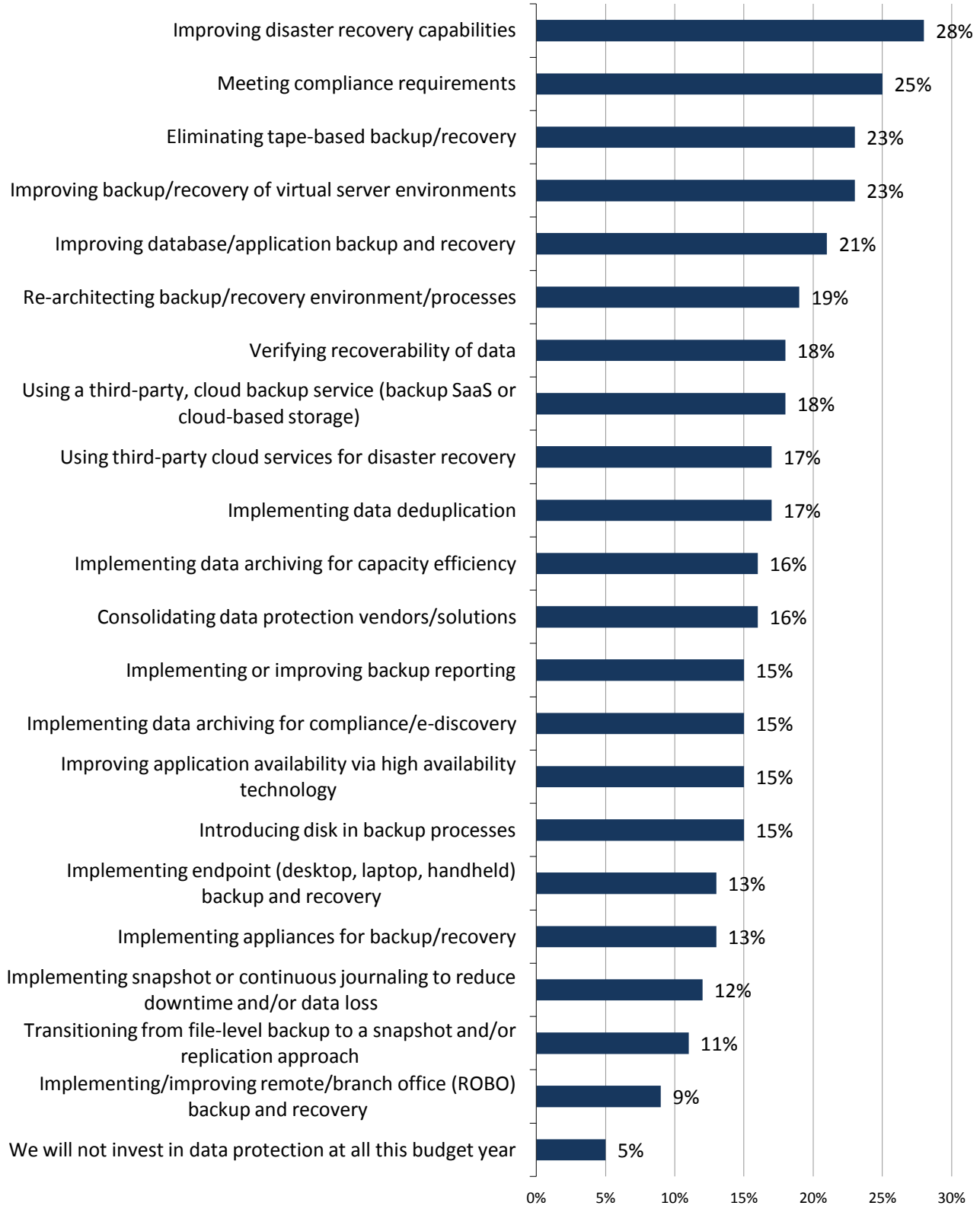
Which of the following would you characterize as challenges with your organization's current data protection processes and technologies? Which would you characterize as the primary challenge for your organization? (Percent of respondents, N=330)



Source: Enterprise Strategy Group, 2012.

Figure 4. Top Areas of Data Protection Investment

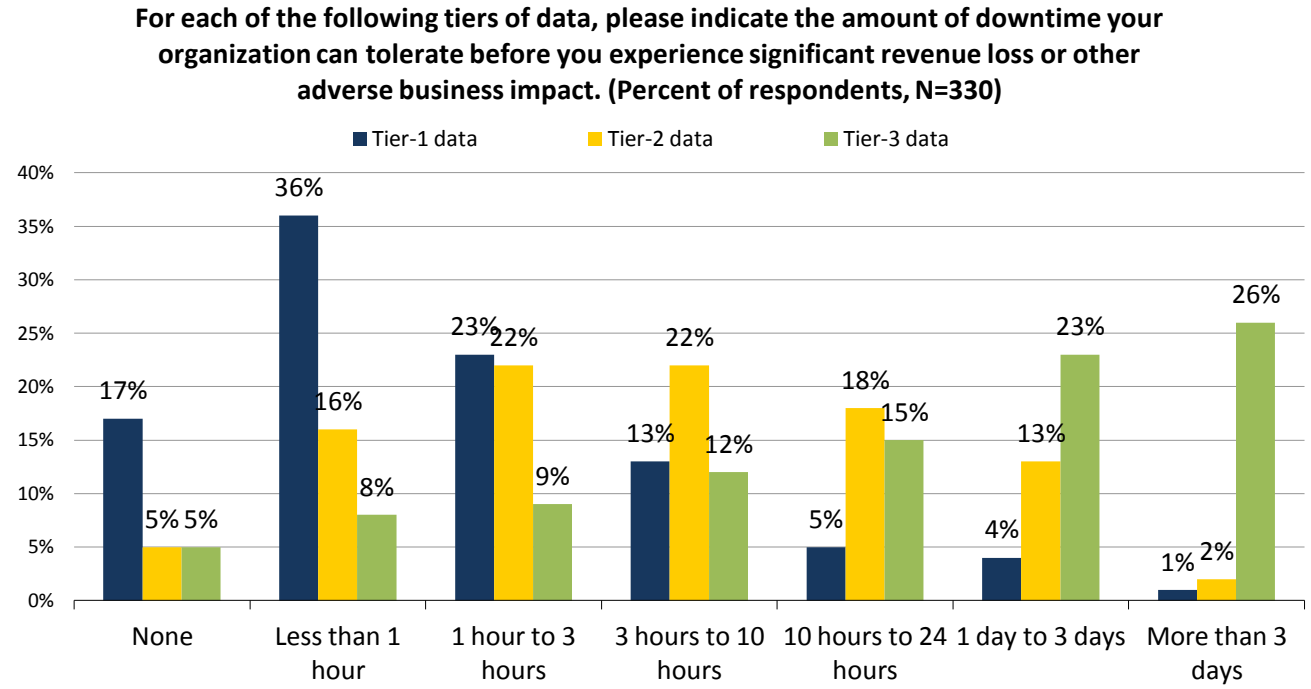
In which areas of data protection do you believe your organization is likely to make the most significant investments over the next 12-18 months? (Percent of respondents, N=330)



Source: Enterprise Strategy Group, 2012.

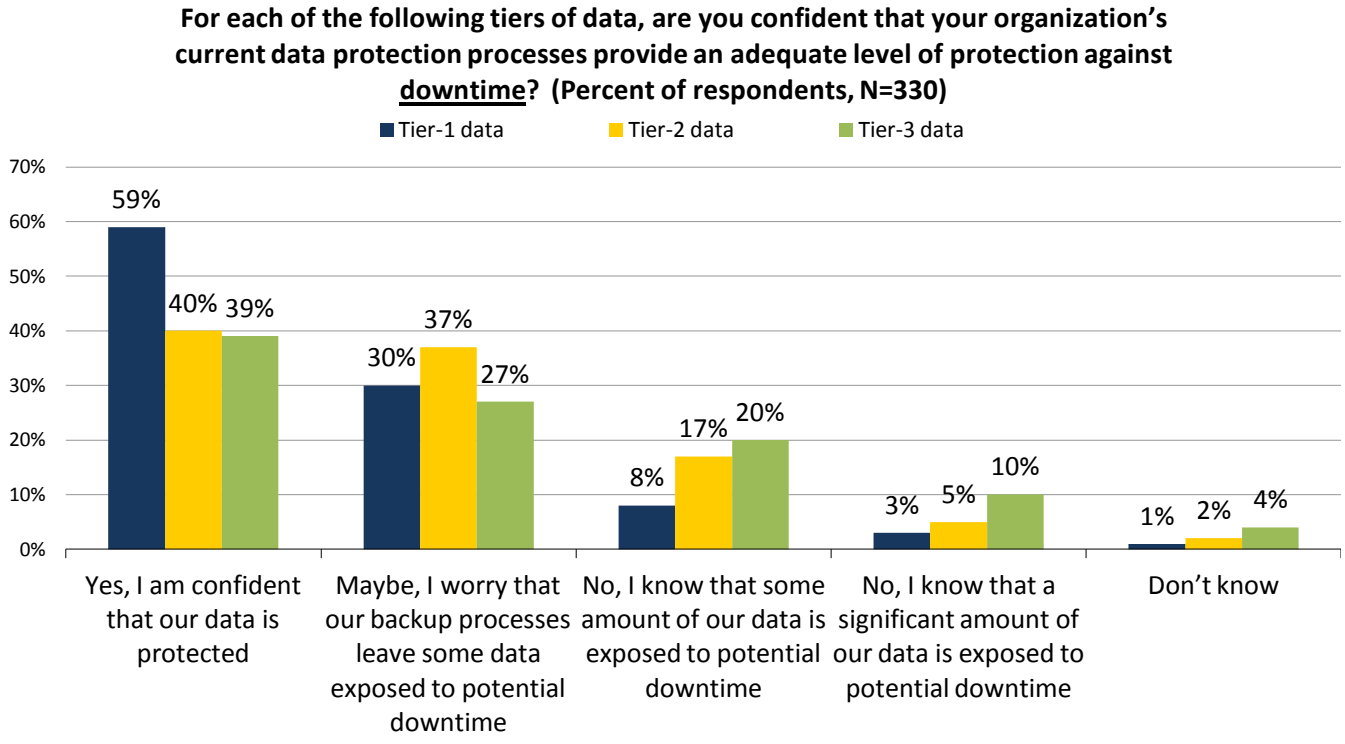
Business Value of Data and the Impact on Data Protection

Figure 5. Amount of Downtime Tolerance



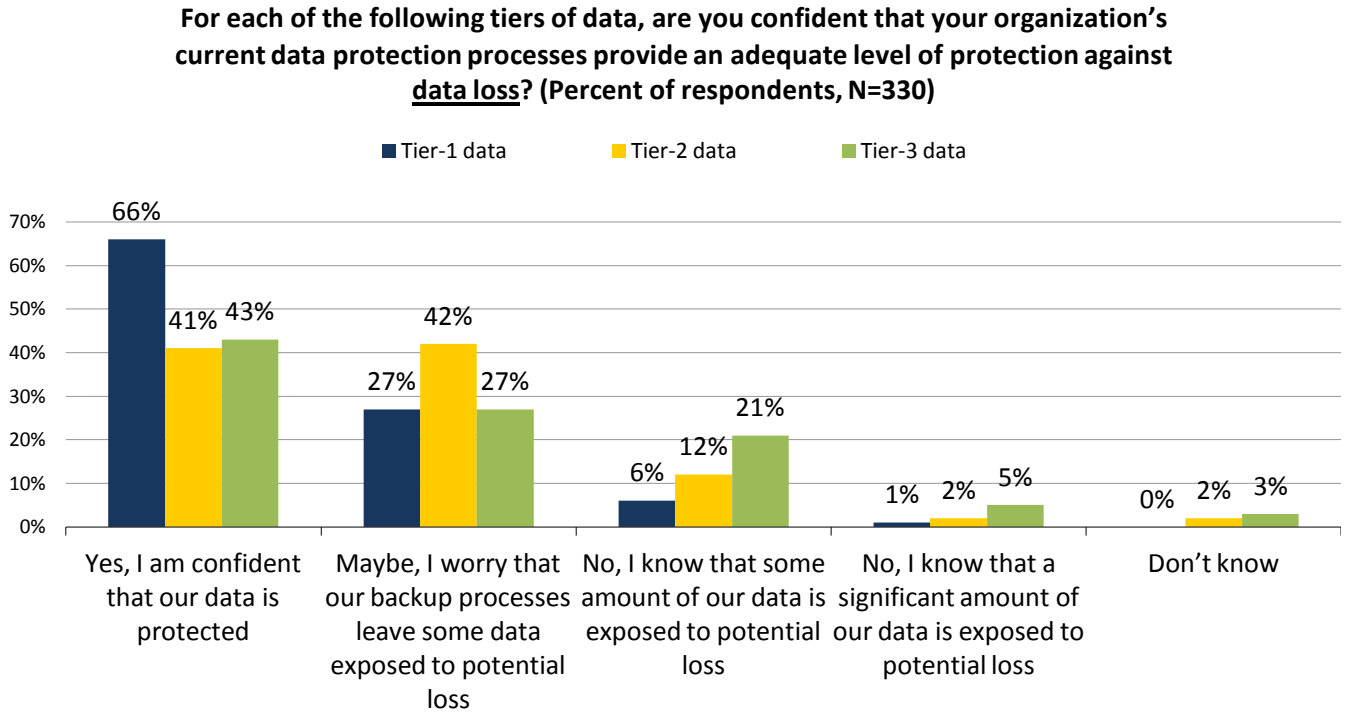
Source: Enterprise Strategy Group, 2012.

Figure 6. Confidence Level that Data Protection Processes Prevent Downtime



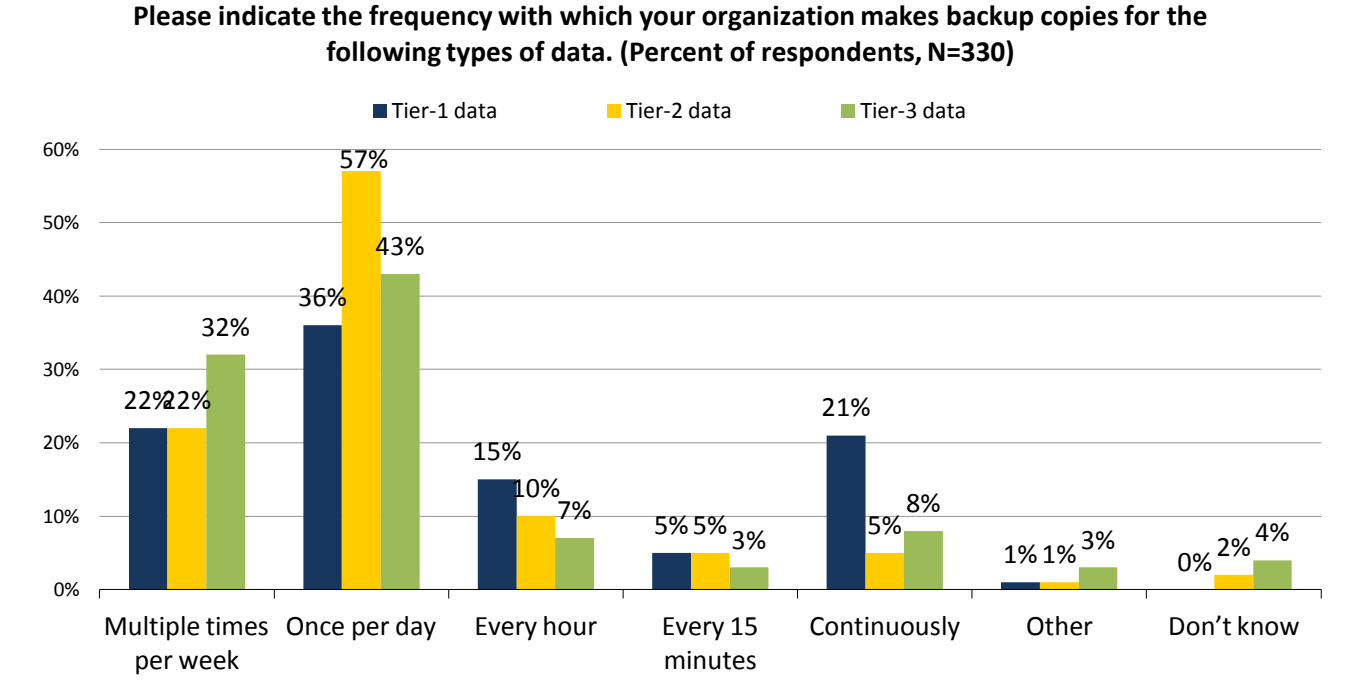
Source: Enterprise Strategy Group, 2012.

Figure 7. Confidence Level that Data Protection Processes Prevent Data Loss



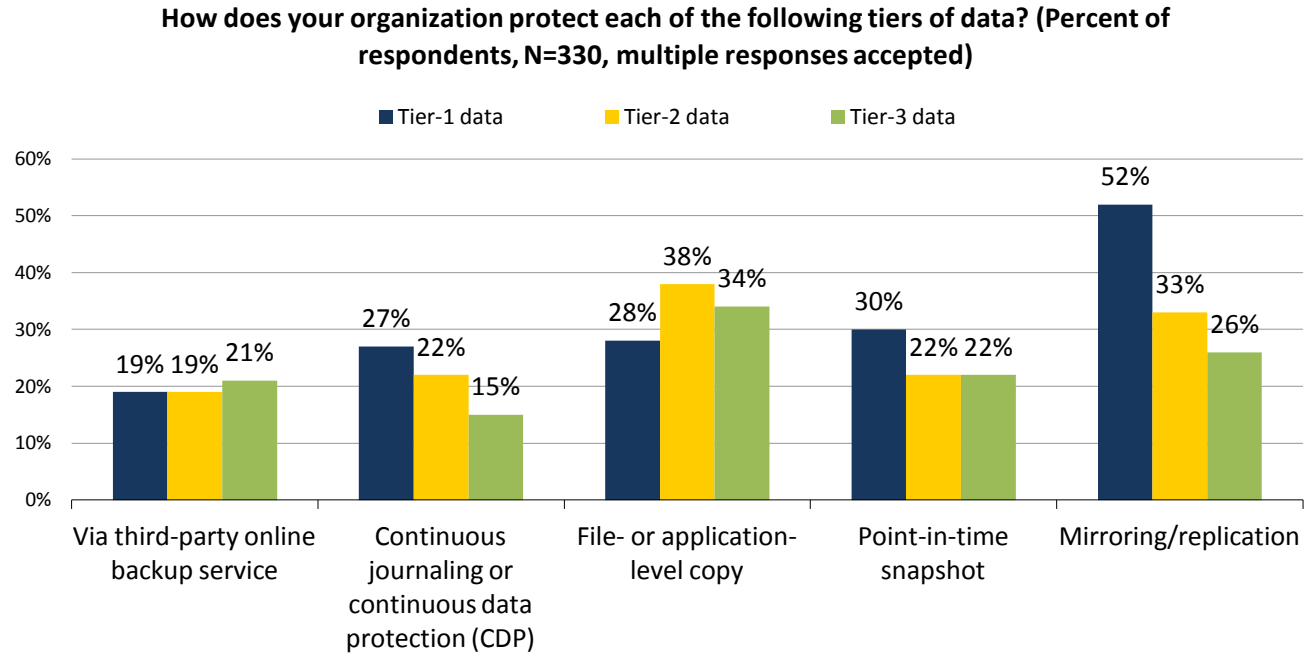
Source: Enterprise Strategy Group, 2012.

Figure 8. Frequency of Backup Copies



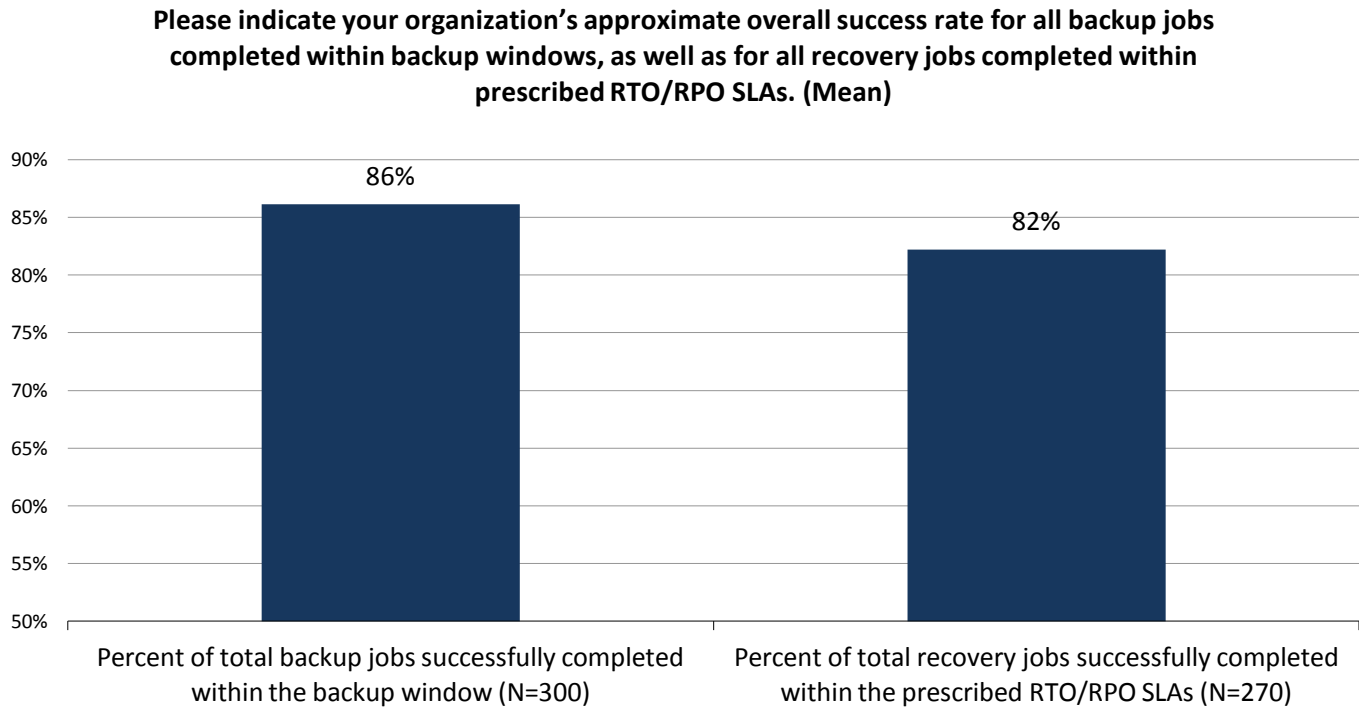
Source: Enterprise Strategy Group, 2012.

Figure 9. Methods of Protecting Data



Source: Enterprise Strategy Group, 2012.

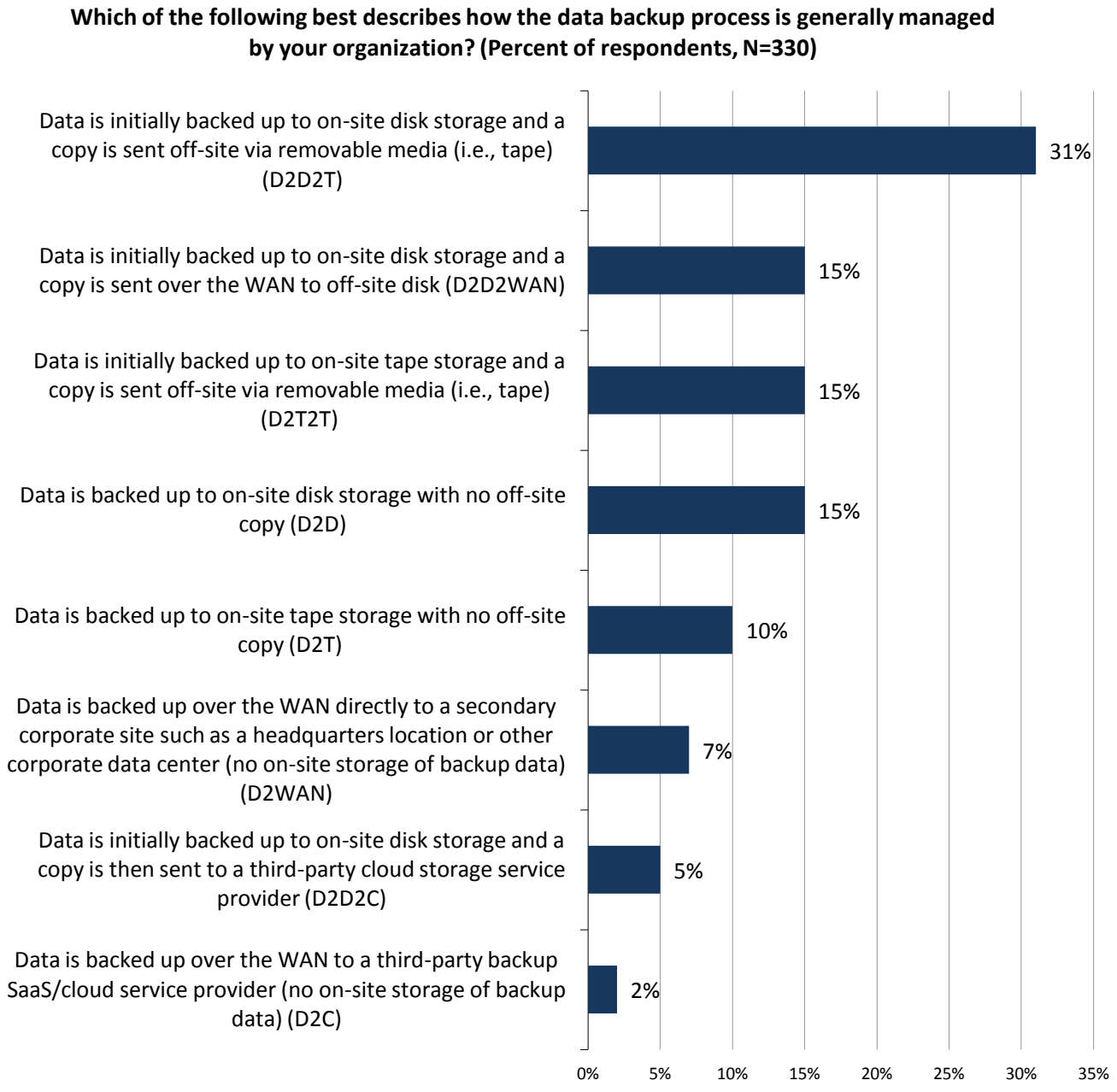
Figure 10. Success Rates for Backup and Recovery Jobs



Source: Enterprise Strategy Group, 2012.

Primary Data Protection Processes

Figure 11. Primary Data Backup Process

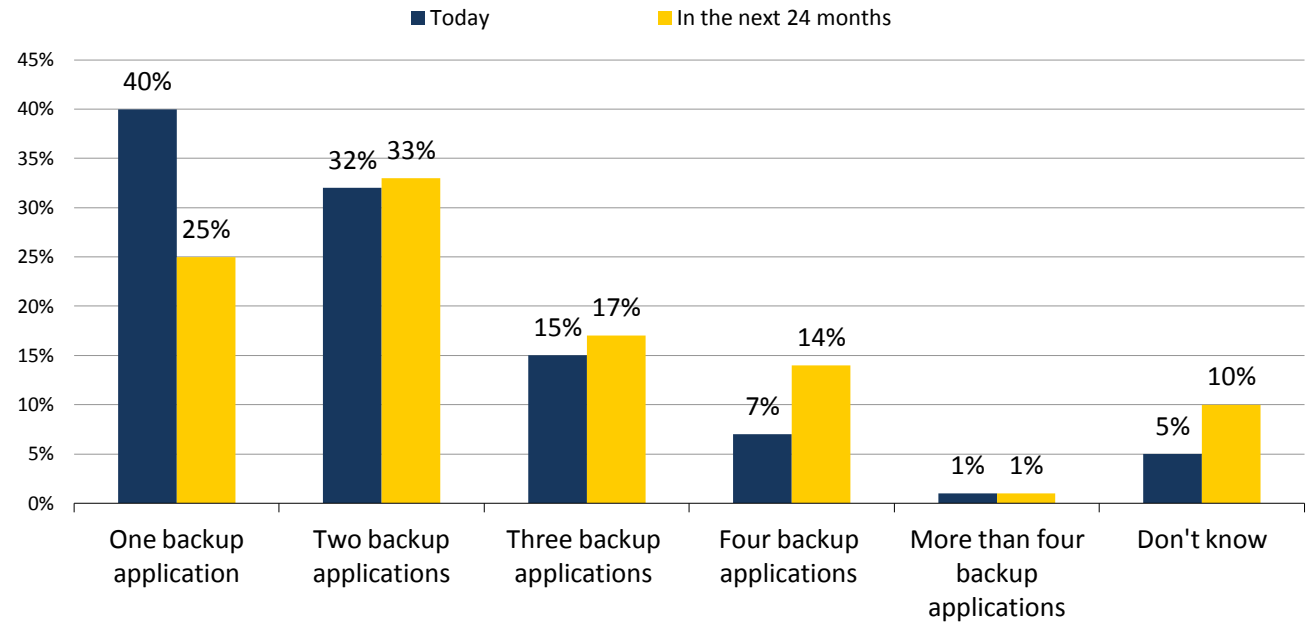


Source: Enterprise Strategy Group, 2012.

Current Backup Environments

Figure 12. Number of Unique Backup Applications Used

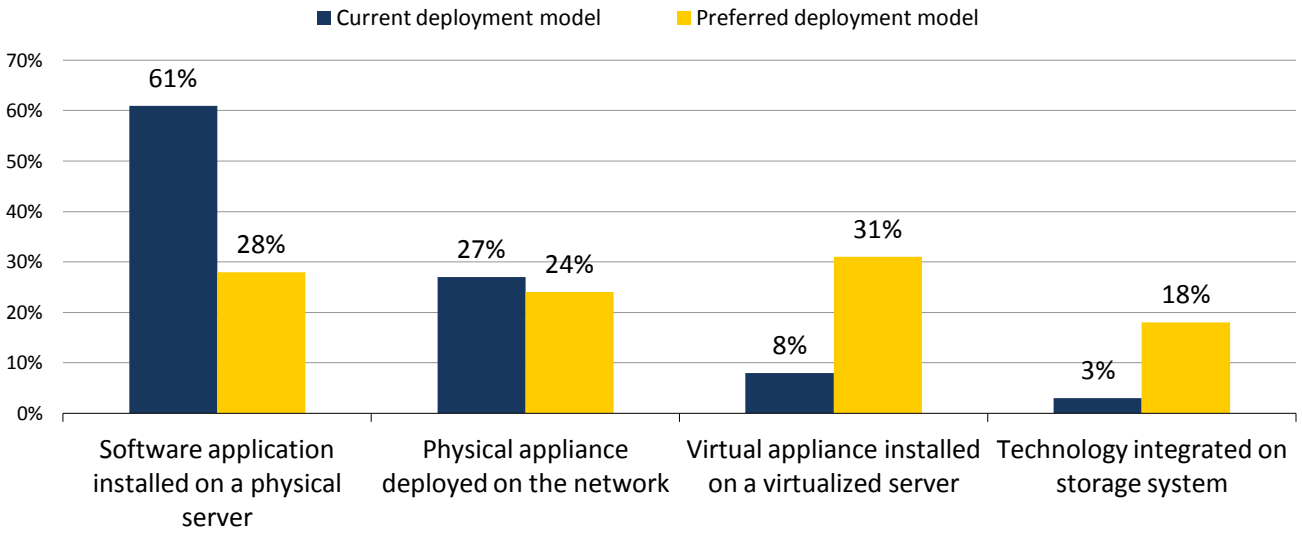
Please indicate the number of unique backup applications in use by your organization (for both physical and virtual environments) today. Indicate how you expect that to change in the next 24 months. (Percent of respondents, N=323)



Source: Enterprise Strategy Group, 2012.

Figure 13. Deployment Model for On-Premises Backup Solution: Current vs. Preferred

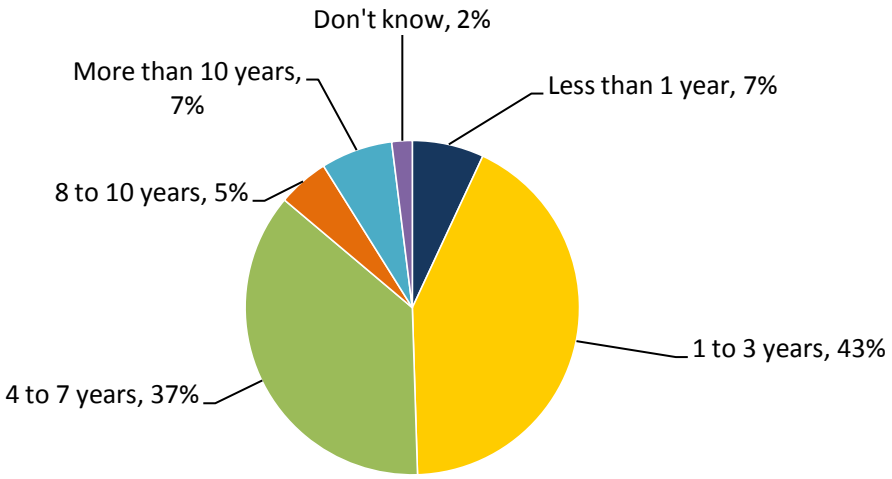
What is your organization's most common deployment model for on-premises backup solutions? Going forward, what would you say is your organization's preference for deploying on-premises backup solutions? (Percent of respondents, N=323)



Source: Enterprise Strategy Group, 2012.

Figure 14. Length of Primary Backup Application Deployment

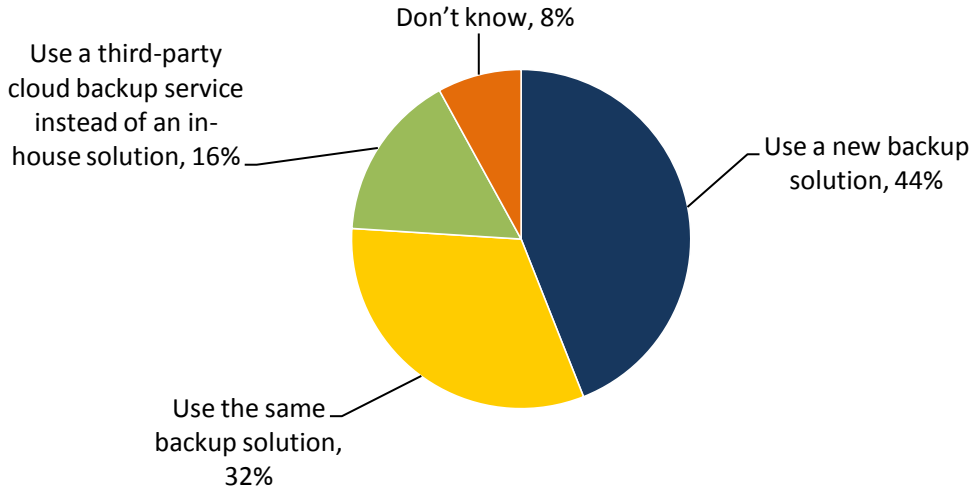
How long has your organization's current primary backup application (regardless of version) been deployed ? (Percent of respondents, N=323)



Source: Enterprise Strategy Group, 2012.

Figure 15. Commitment to Current Backup Process

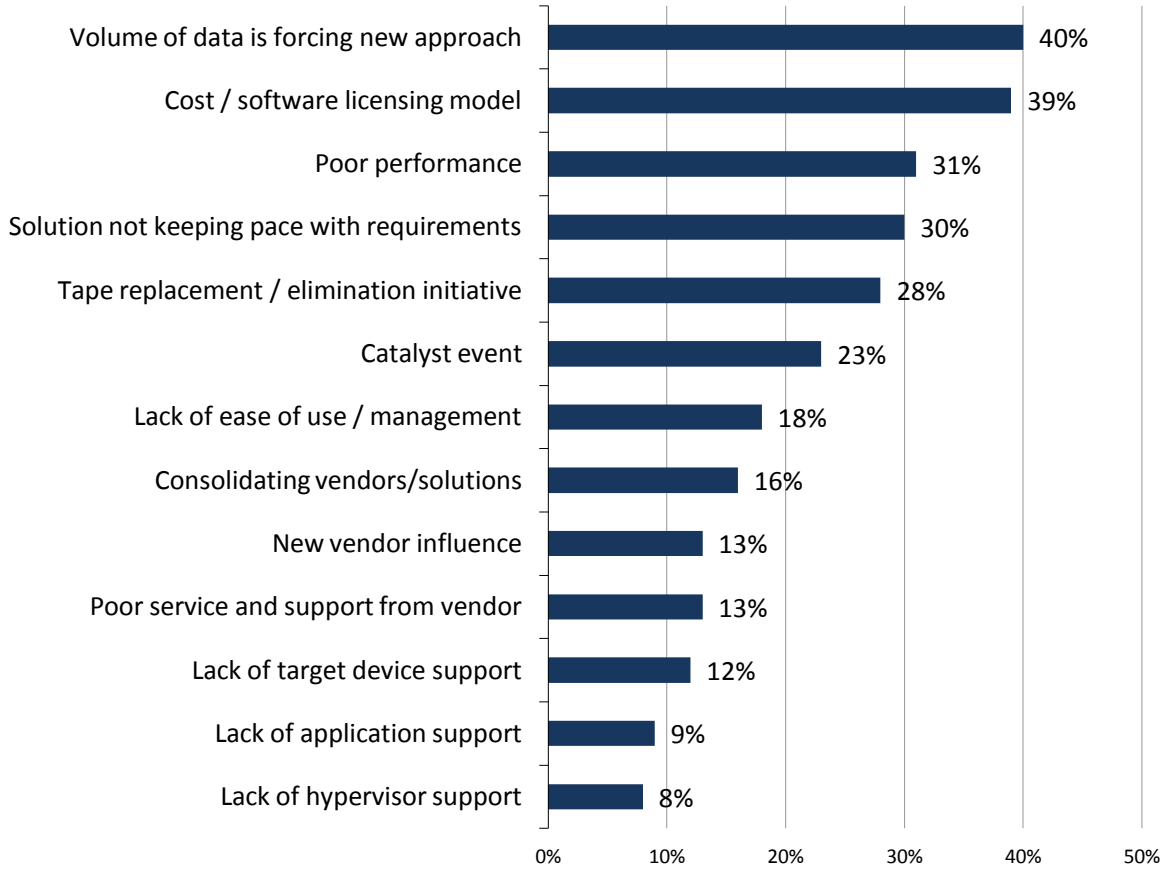
If provided the opportunity to completely re-architect its backup process(es) from scratch, do you believe your organization would: (Percent of respondents, N=323)



Source: Enterprise Strategy Group, 2012.

Figure 16. Factors Most Likely to Drive Replacement of Current Backup Solution

Which of the following factors do you believe would be most likely to drive your organization to replace its current backup solution? (Percent of respondents, N=142, multiple responses accepted)

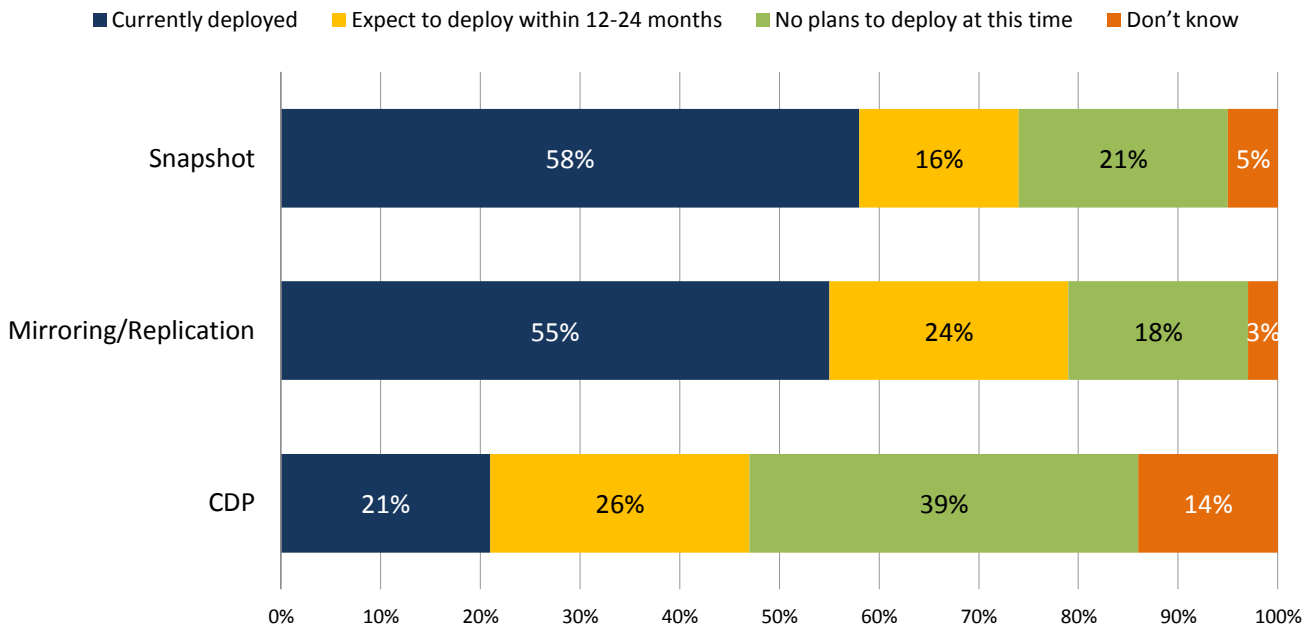


Source: Enterprise Strategy Group, 2012.

Adoption of Alternative Data Protection Technologies

Figure 17. Usage of Data Protection Technologies to Back Up Data on Physical Servers

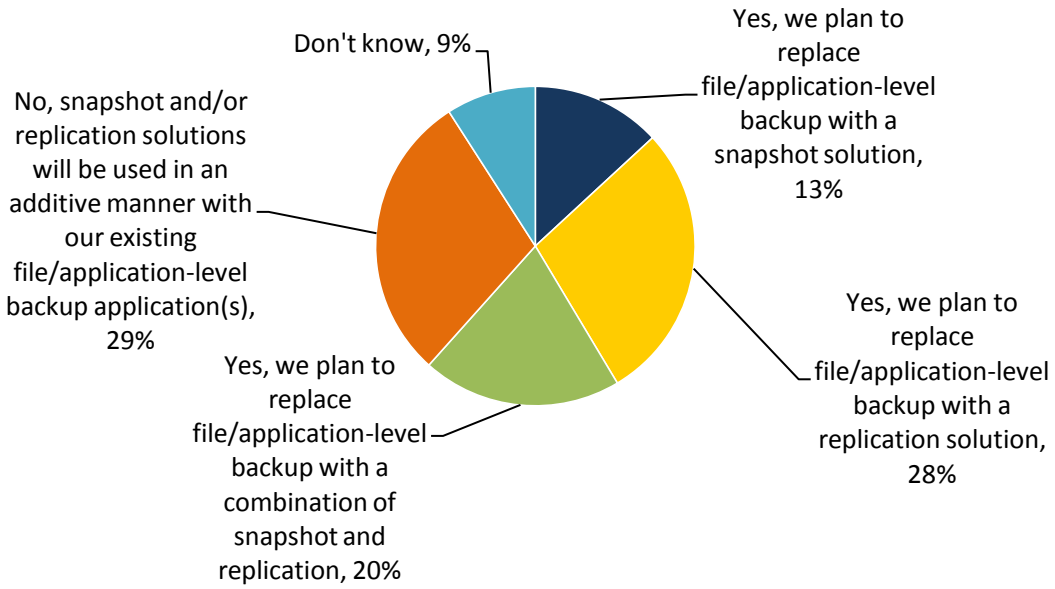
Please describe your organization's current or planned usage of the following data protection technologies to back up data on its physical servers. (Percent of respondents, N=323)



Source: Enterprise Strategy Group, 2012.

Figure 18. Plans to Replace File/Application Level Backup with a Snapshot or Replication Solution

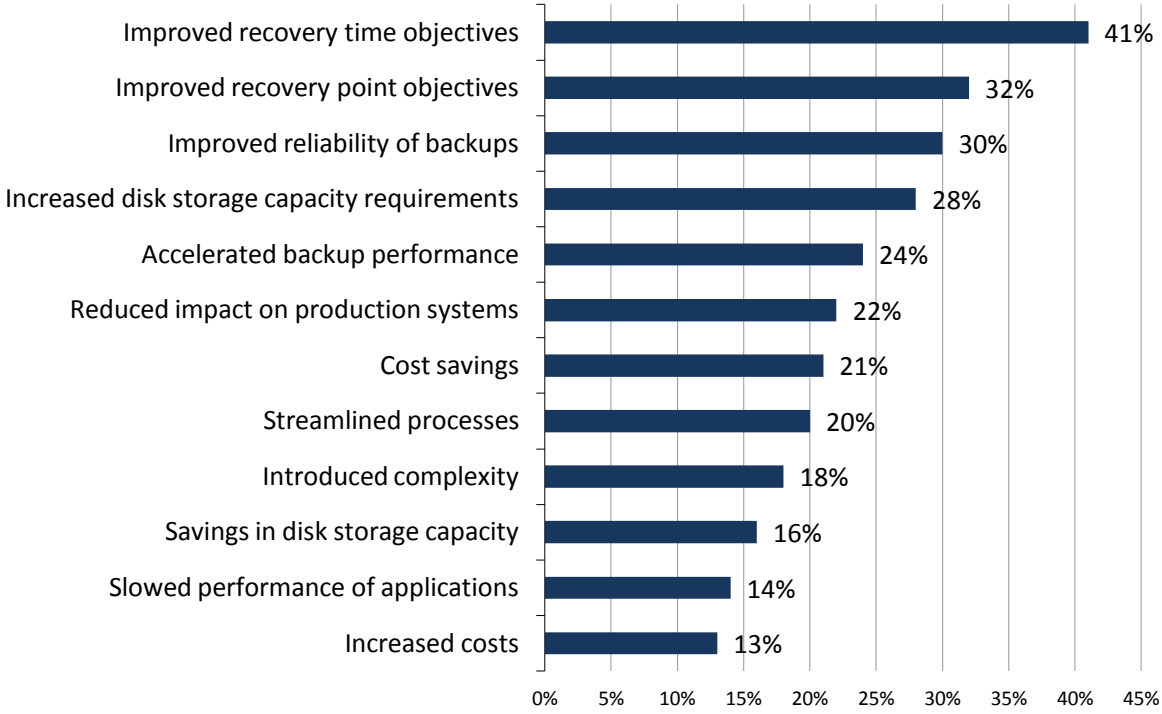
To the best of your knowledge, does your organization have plans to replace all or some file/application-level backup with a snapshot or replication solution? (Percent of respondents, N=181)



Source: Enterprise Strategy Group, 2012.

Figure 19. Impact of Snapshot Technology on Data Protection Processes

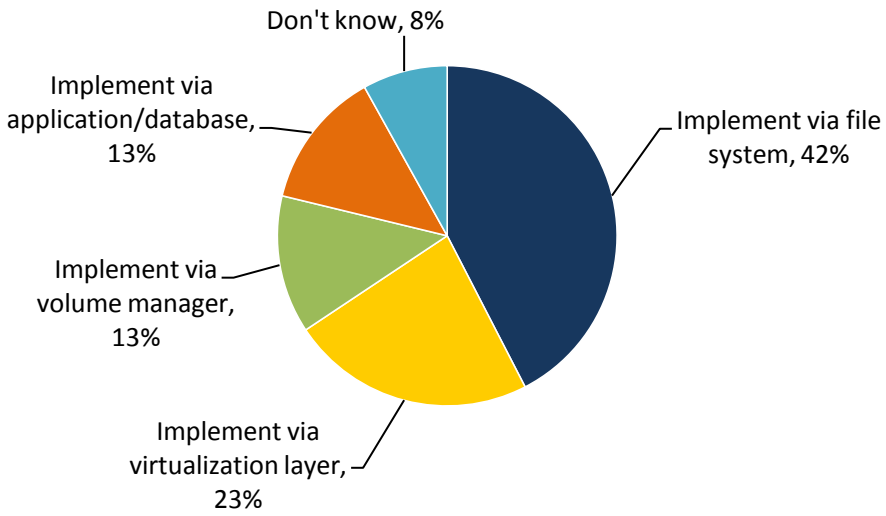
How has the implementation of snapshot technology impacted your organization's data protection processes? (Percent of respondents, N=187, multiple responses accepted)



Source: Enterprise Strategy Group, 2012.

Figure 20. Expected Implementation of Snapshot Technology

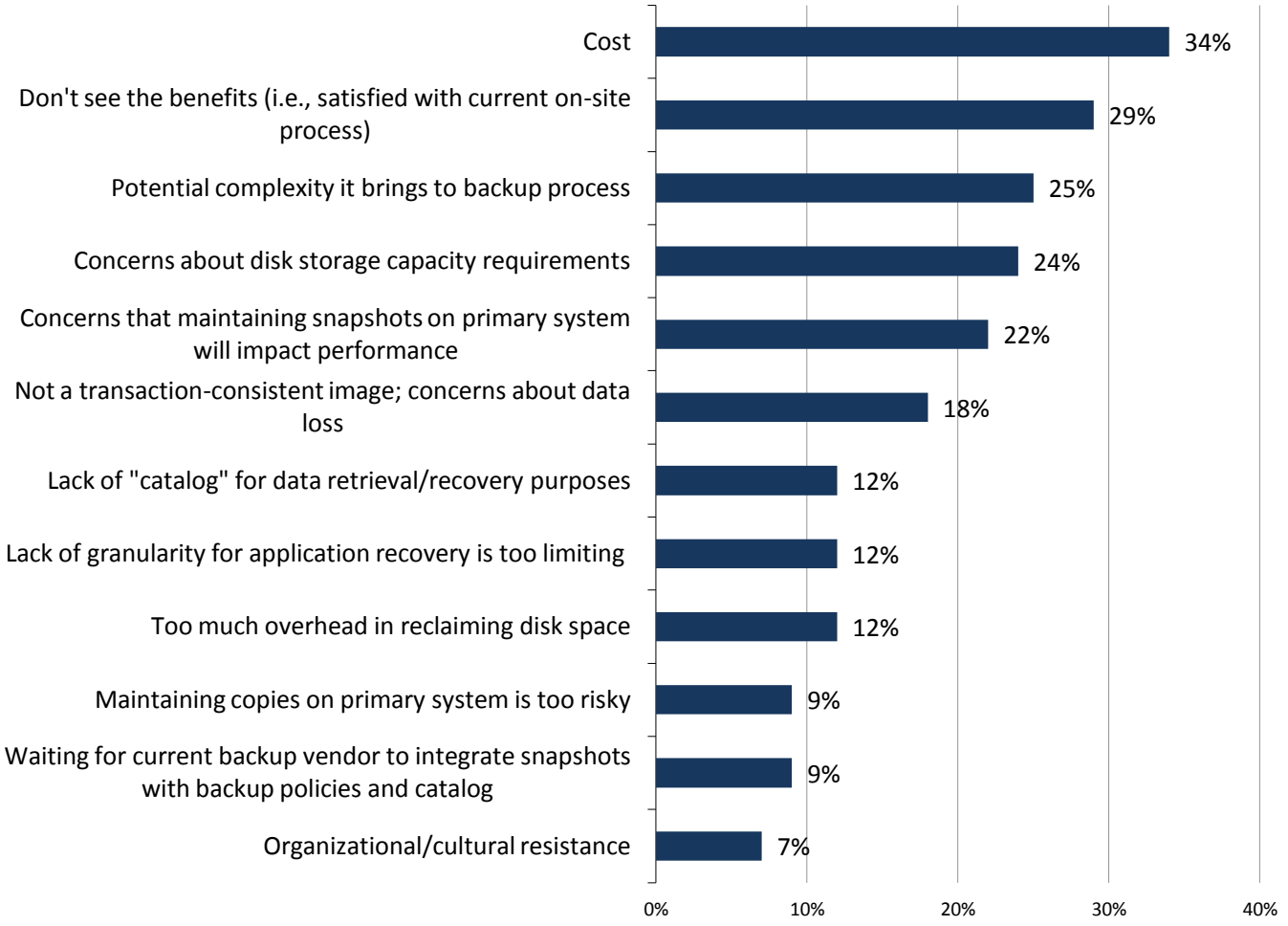
How do you expect your organization will implement snapshot technology? (Percent of respondents, N=52)



Source: Enterprise Strategy Group, 2012.

Figure 21. Reasons Why Organizations Have No Plans to Use Snapshot Technology

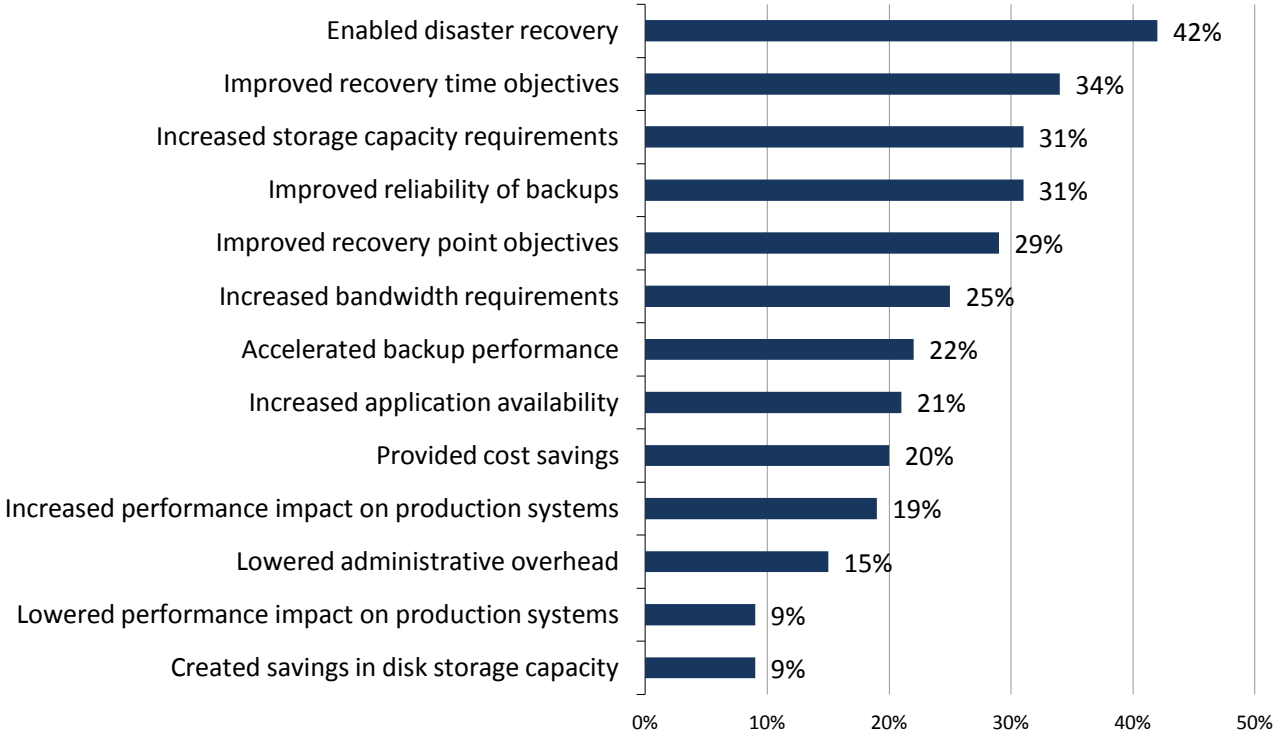
To the best of your knowledge, why do you believe your organization has no plans to utilize snapshot technology for physical system backup operations? (Percent of respondents, N=68, multiple responses accepted)



Source: Enterprise Strategy Group, 2012.

Figure 22. Impact of Replication on Data Protection Processes

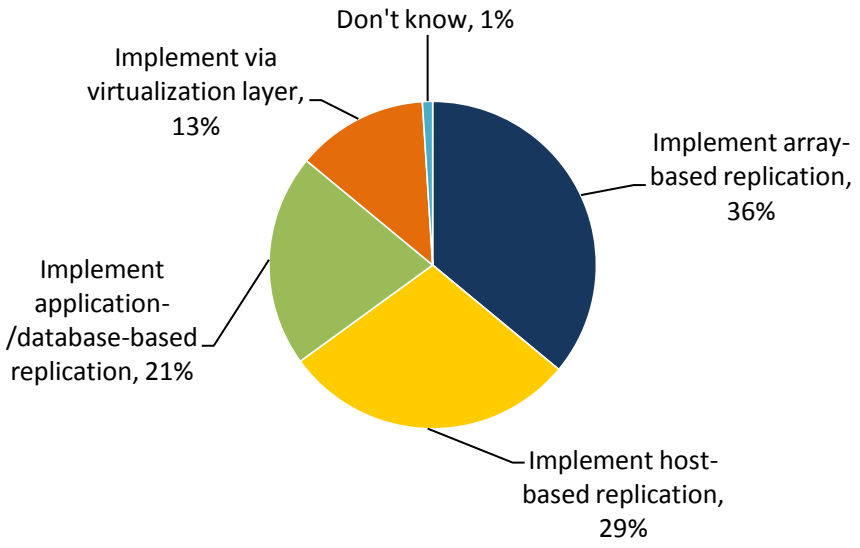
How has the implementation of replication technology impacted your organization's data protection processes? (Percent of respondents, N=178, multiple responses accepted)



Source: Enterprise Strategy Group, 2012.

Figure 23. Expected Implementation of Replication Technology

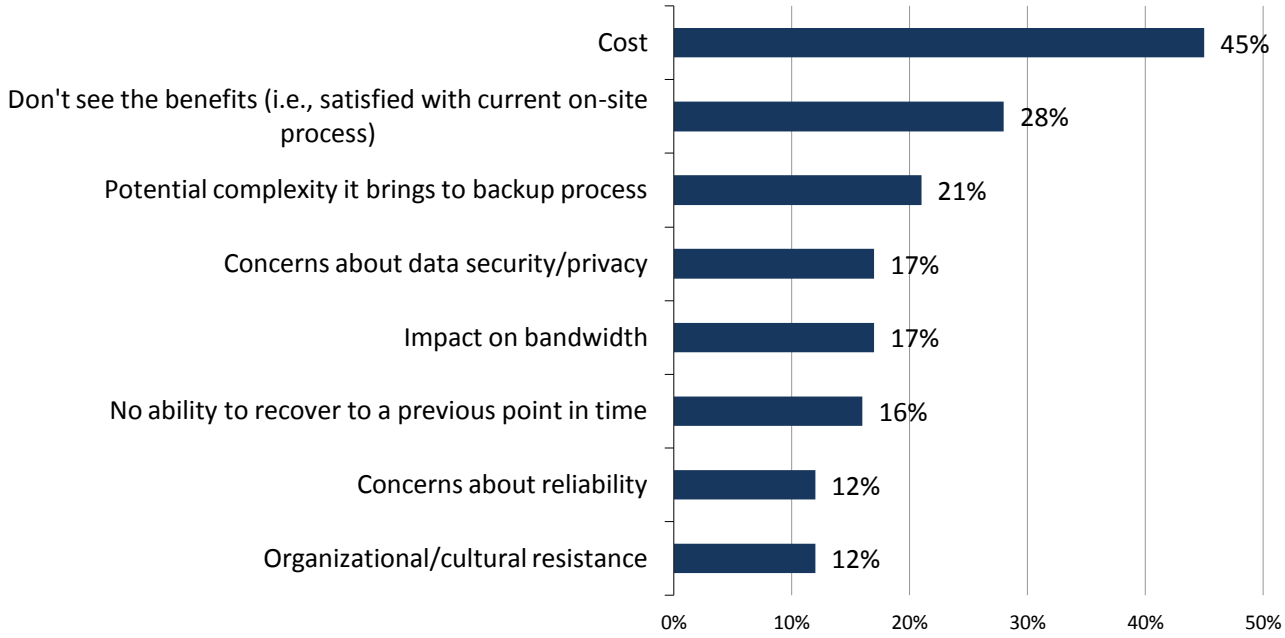
How do you expect your organization will implement replication technology? (Percent of respondents, N=78)



Source: Enterprise Strategy Group, 2012.

Figure 24. Reasons Why Organizations Have No Plans to Use Replication Technology

To the best of your knowledge, why do you believe your organization has no plans to utilize replication technology for physical system backup operations? (Percent of respondents, N=58, multiple responses accepted)

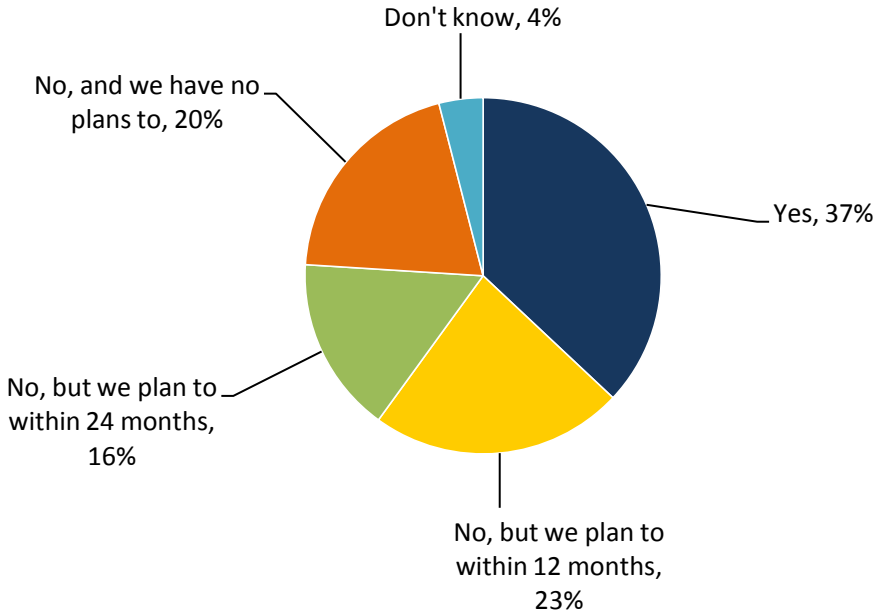


Source: Enterprise Strategy Group, 2012.

Deduplication Technology

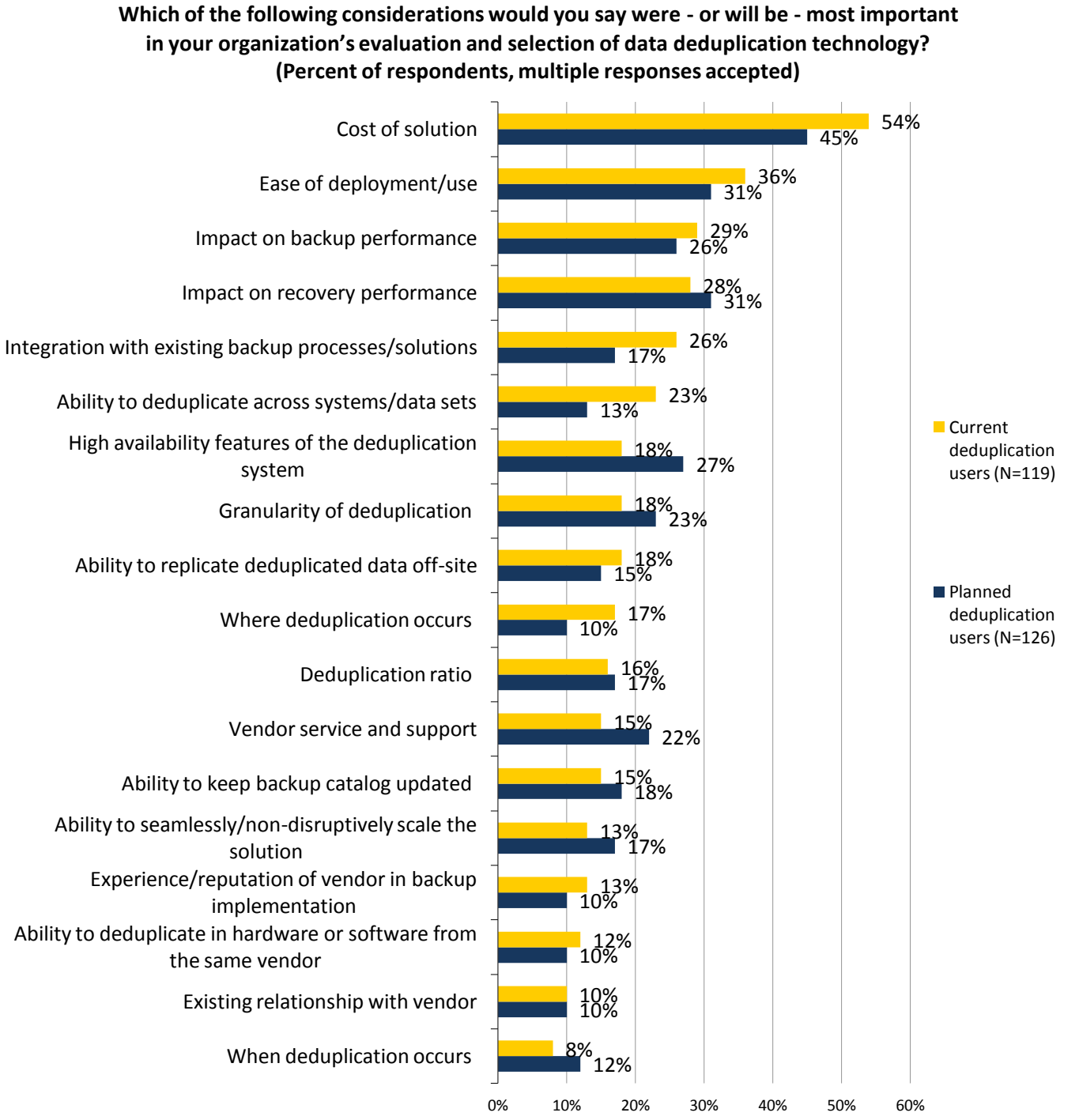
Figure 25. Use of Data Deduplication

Is your organization currently using any data deduplication solutions? (Percent of respondents, N=323)



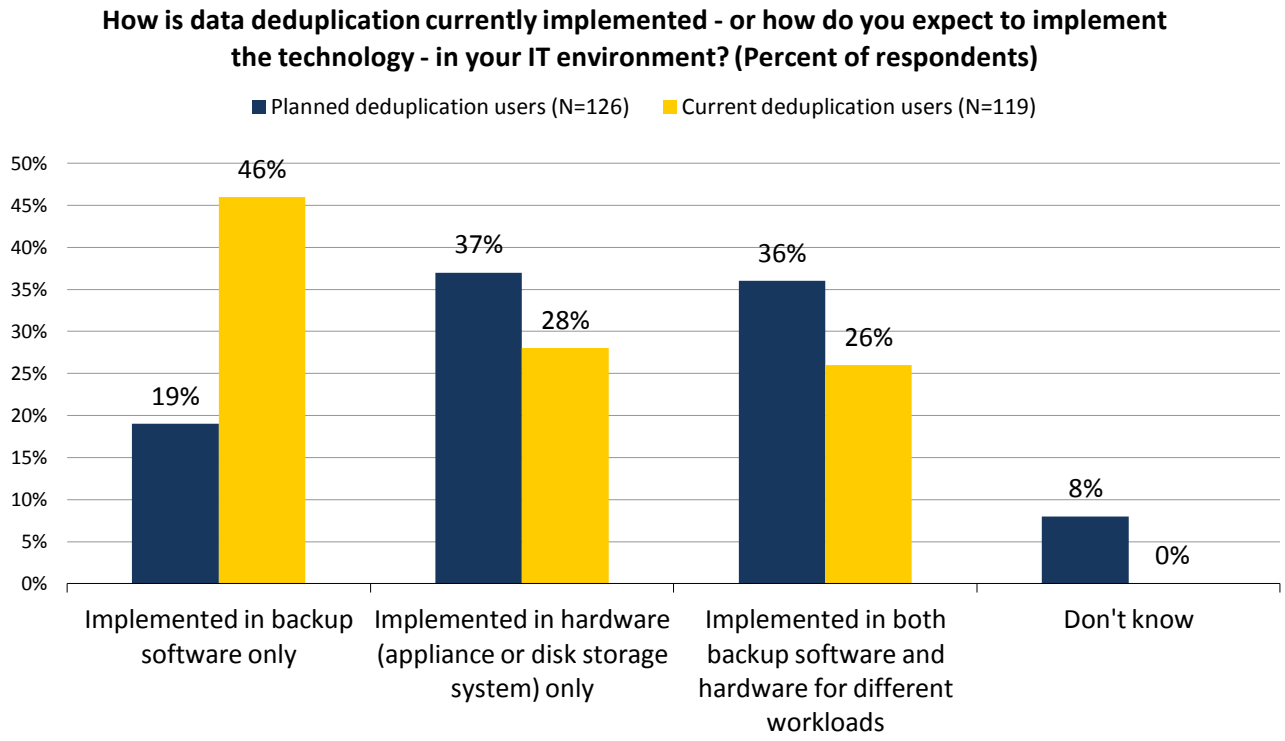
Source: Enterprise Strategy Group, 2012.

Figure 26. Most Important Considerations When Evaluating and Selecting Deduplication Technology: Current vs. Planned Users



Source: Enterprise Strategy Group, 2012.

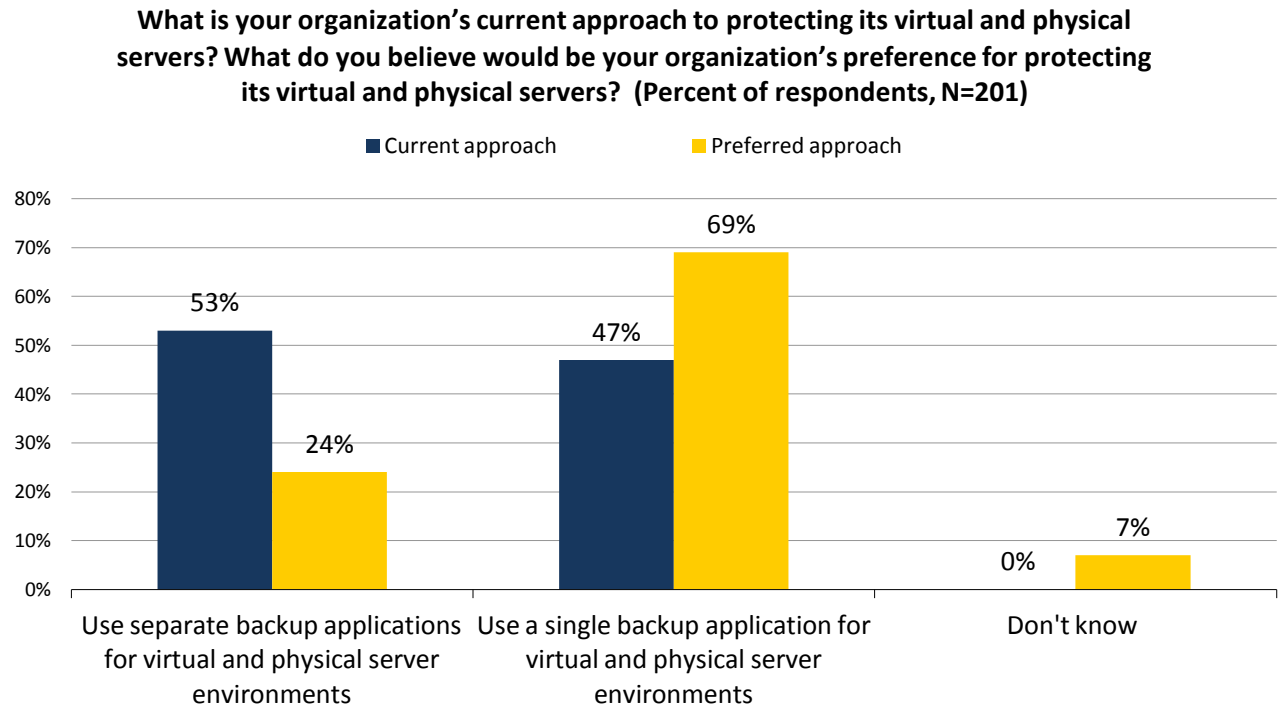
Figure 27. Data Deduplication Implementation Models: Current vs. Planned Users



Source: Enterprise Strategy Group, 2012.

Protecting Virtual Environments

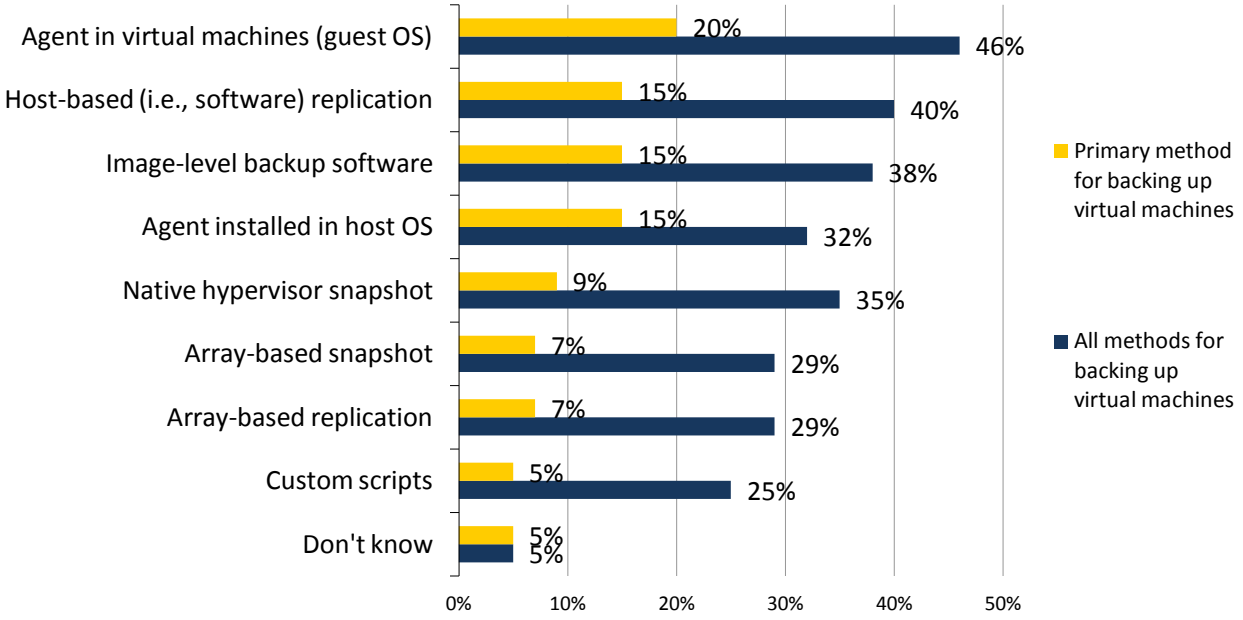
Figure 28. Approach to Protecting Virtual and Physical Servers



Source: Enterprise Strategy Group, 2012.

Figure 29. Approaches to Protecting Virtual Machines

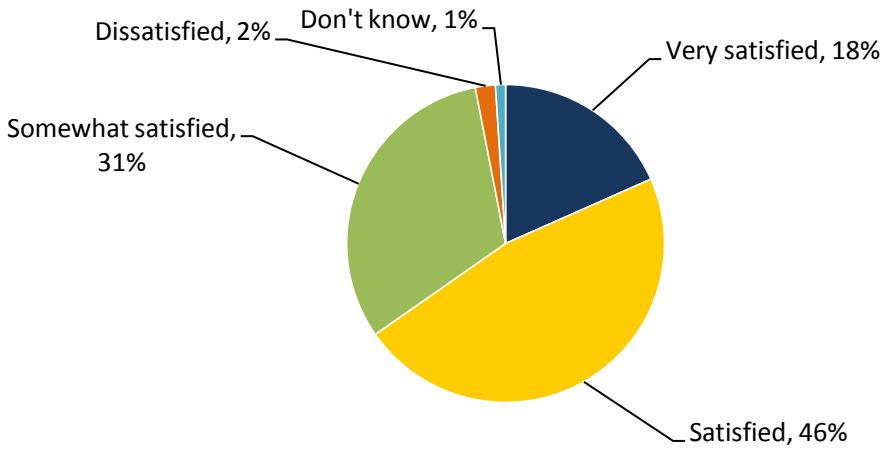
Which of the following approaches does your organization utilize to back up its virtual machines/instances? (Percent of respondents, N=201)



Source: Enterprise Strategy Group, 2012.

Figure 30. Level of Satisfaction with Primary Method of Backing Up Virtual Machines

What is your organization's level of satisfaction with its primary method for backing up virtual machines? (Percent of respondents, N=201)

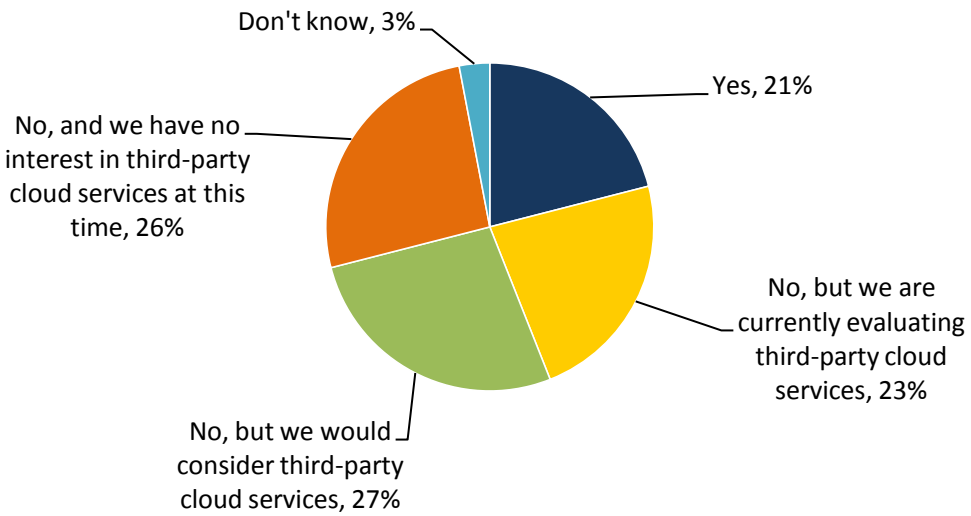


Source: Enterprise Strategy Group, 2012.

Using the Cloud for Data Protection

Figure 31. Utilization of Third-Party Cloud Services for Data Protection

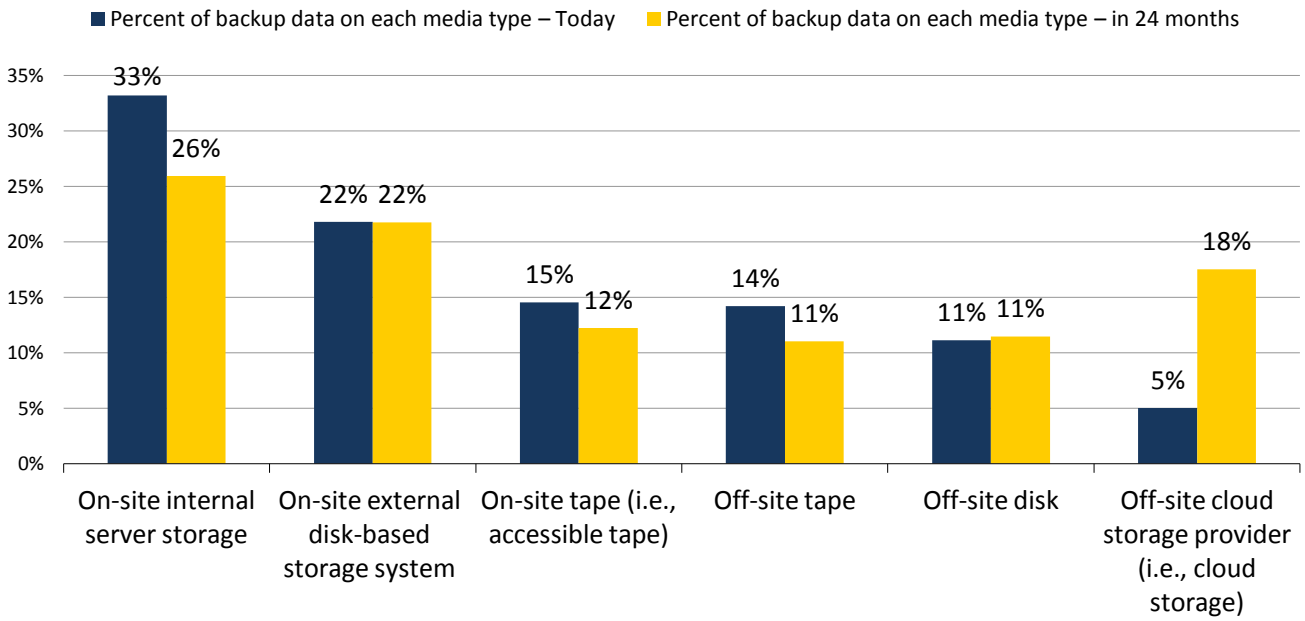
To the best of your knowledge, does your organization currently utilize third-party cloud services for any data protection (i.e., backup, DR) operations? (Percent of respondents, N=323)



Source: Enterprise Strategy Group, 2012.

Figure 32. Significant Shift of Backup Data to the Cloud over the Next Two Years

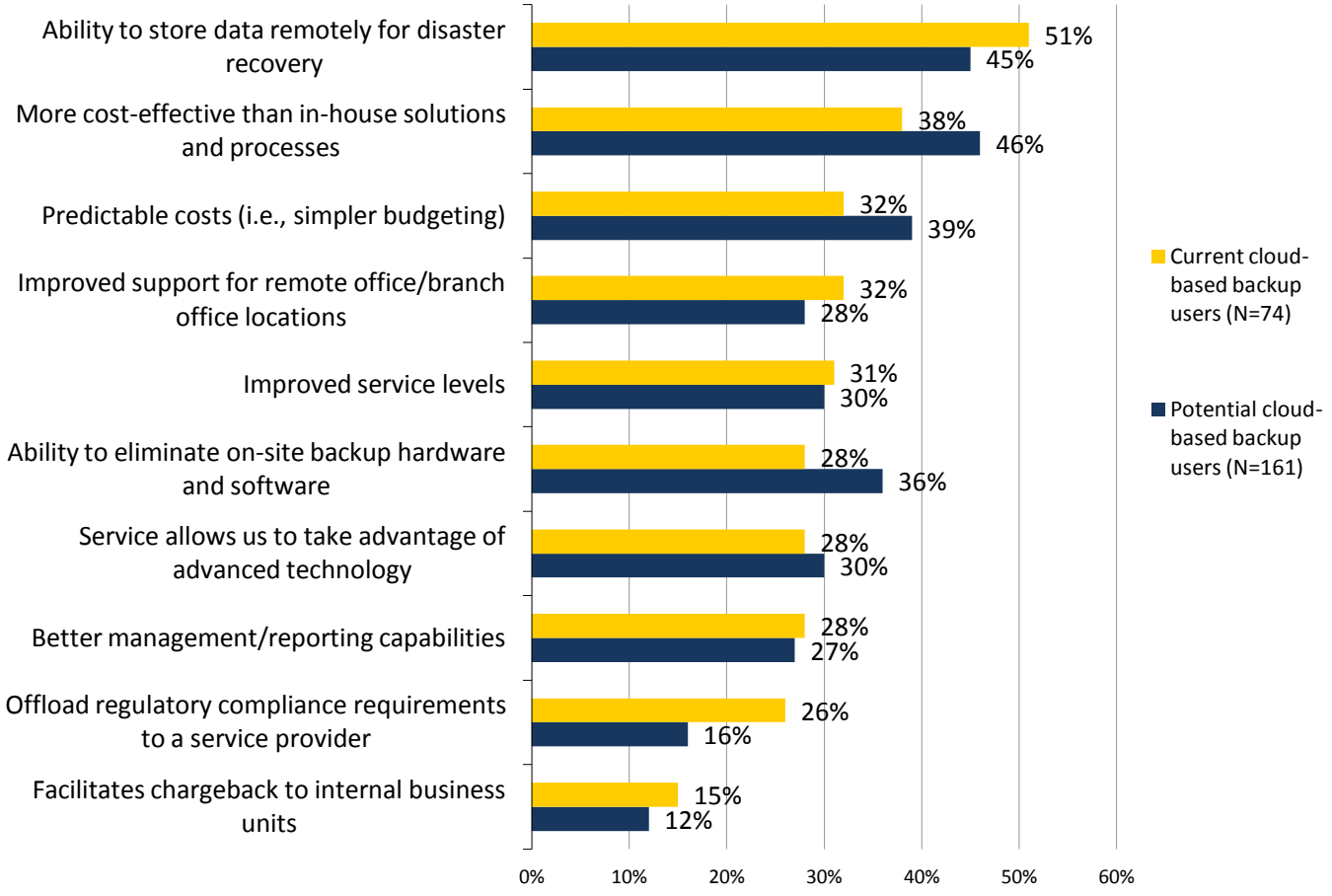
Approximately what percentage of your organization's total volume of backup data is currently stored on each of the following storage media types? Please also indicate what you expect these percentages to be in the next 24 months. (Mean, N=330)



Source: Enterprise Strategy Group, 2012.

Figure 33. Factors Driving Decision to Use Cloud-based Backup Service: Current vs. Potential Users

Which of the following factors do you believe would be most likely to lead your organization to utilize - or consider - a cloud backup service? (Percent of respondents, multiple responses accepted)



Source: Enterprise Strategy Group, 2012.

Research Methodology

To gather data for this report, ESG conducted a comprehensive online survey of IT managers from private- and public-sector organizations in North America (United States and Canada) and Western Europe (United Kingdom, France, and Germany) between January 9, 2012 and January 27, 2012. To qualify for this survey, respondents were required to be senior IT managers familiar with and/or personally responsible for evaluating, purchasing, or managing data protection technologies—such as backup and recovery software, data replication software, and disk or tape storage systems used for secondary data storage—for their organization.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 330 IT managers.

Please see the *Respondent Demographics* section of this report for more information on these respondents.

Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

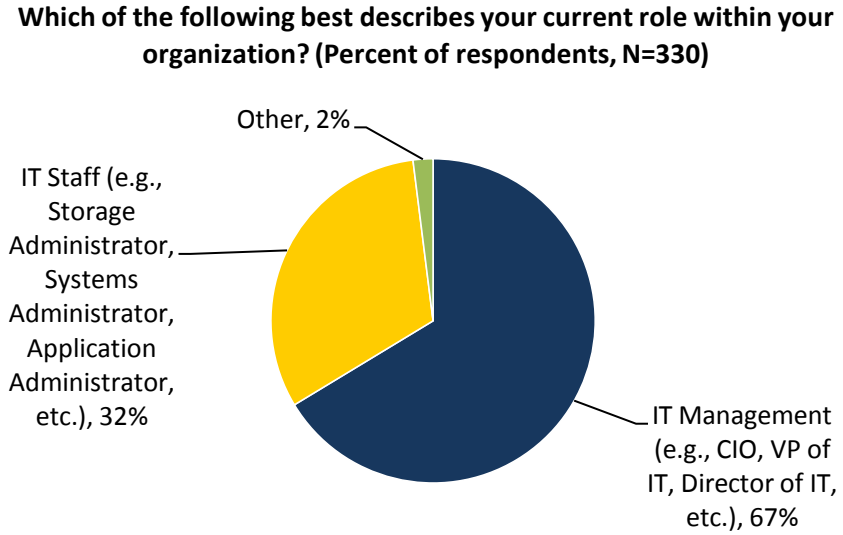
Respondent Demographics

The data presented in this report is based on a survey of 330 qualified respondents. The figures below detail the demographics of the respondent base, including individual respondents' current job responsibility and technology area of responsibility, total number of employees, primary industry, annual revenue, total number of production servers, and total volume of data.

Respondents by Role

The breakdown of current roles within an organization among survey respondents is shown in Figure 34.

Figure 34. Survey Respondents, by Role

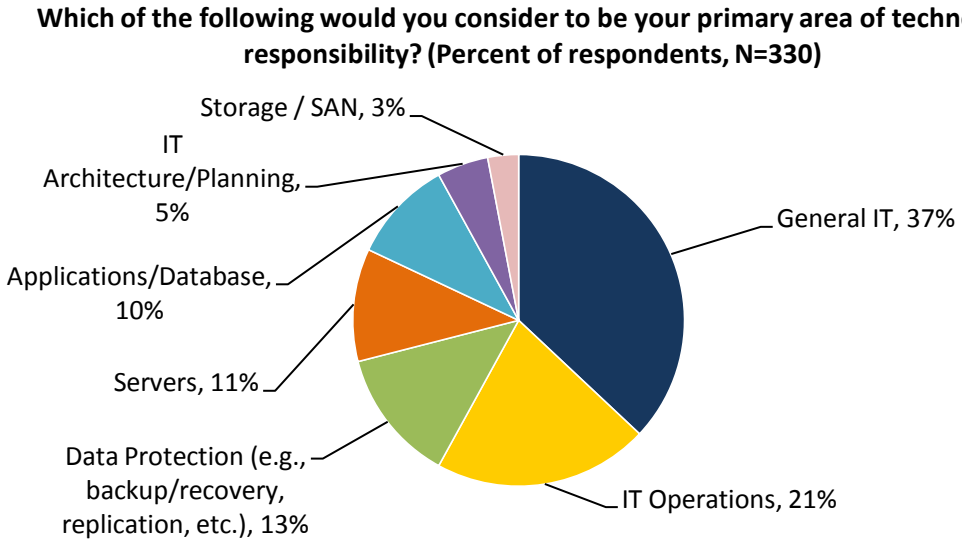


Source: Enterprise Strategy Group, 2012.

Respondents by Primary Technology Responsibility

Respondents' primary area of technology responsibility is shown in Figure 35.

Figure 35. Survey Respondents, by Primary Technology Responsibility



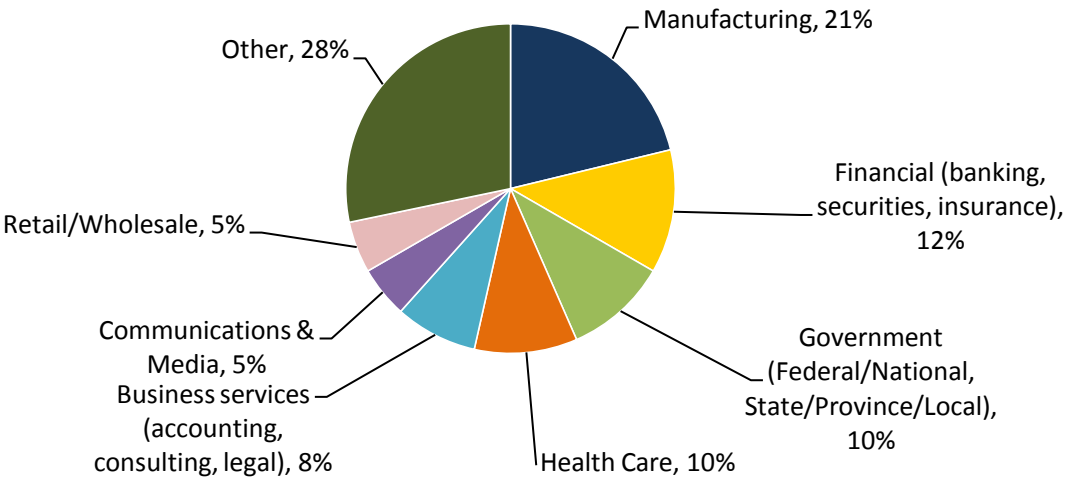
Source: Enterprise Strategy Group, 2012.

Respondents by Industry

Respondents were asked to identify their organization's primary industry. In total, ESG received completed, qualified responses from individuals in 19 distinct vertical industries, plus an "Other" category. Respondents were then grouped into the broader categories shown in Figure 36.

Figure 36. Survey Respondents, by Industry

What is your organization's primary industry? (Percent of respondents, N=330)



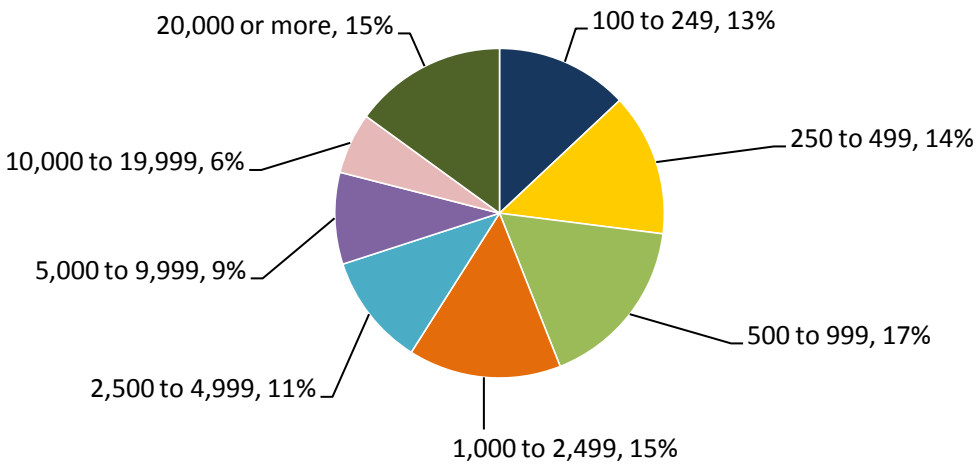
Source: Enterprise Strategy Group, 2012.

Respondents by Number of Employees

The number of employees in respondents' organizations is shown in Figure 37.

Figure 37. Survey Respondents, by Number of Employees

How many total employees does your organization have worldwide? (Percent of respondents, N=330)

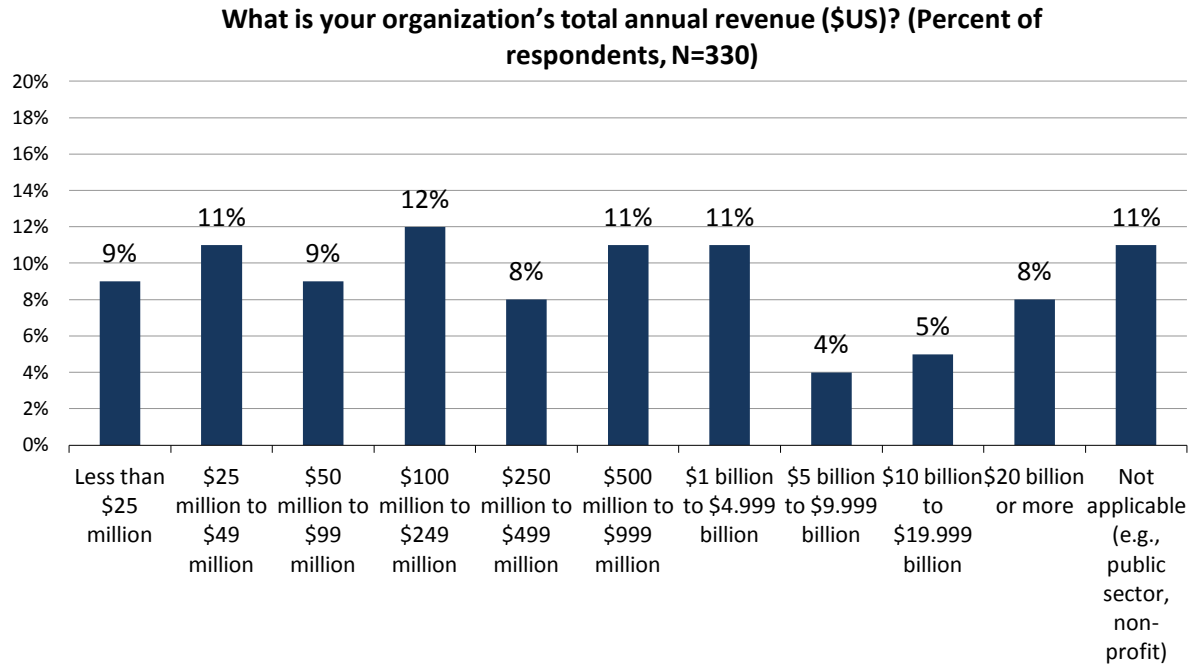


Source: Enterprise Strategy Group, 2012.

Respondents by Annual Revenue

Respondent organizations' annual revenue is shown in Figure 38.

Figure 38. Survey Respondents, by Annual Revenue

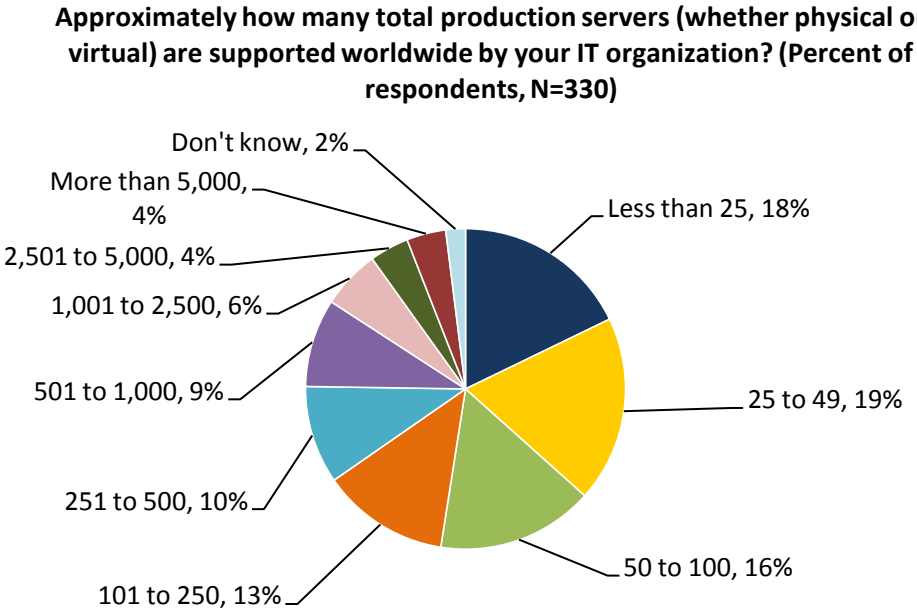


Source: Enterprise Strategy Group, 2012.

Respondents by Number of Production Servers

Respondent organizations' number of production servers is shown in Figure 39.

Figure 39. Survey Respondents, by Number of Production Servers

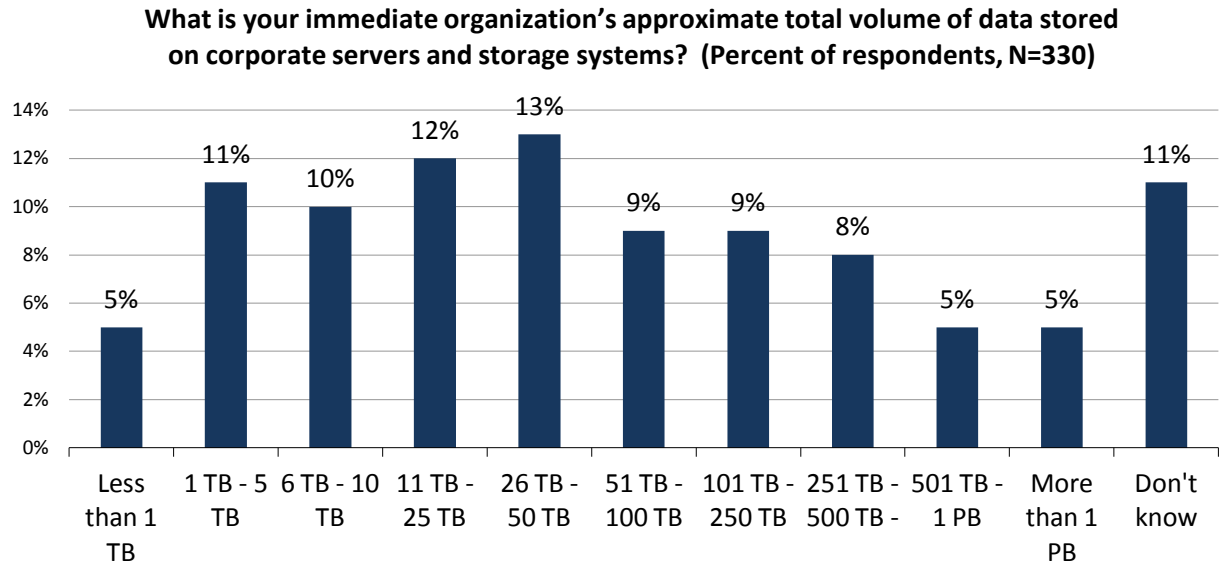


Source: Enterprise Strategy Group, 2012.

Respondents by Total Volume of Data

The approximate total volume of data stored on corporate servers and storage systems in respondents' organizations is shown in Figure 40.

Figure 40. Survey Respondents, by Total Volume of Data



Source: Enterprise Strategy Group, 2012.

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel: 508.482.0188 Fax: 508.482.0128 | www.enterprisestrategygroup.com